The New Data Center

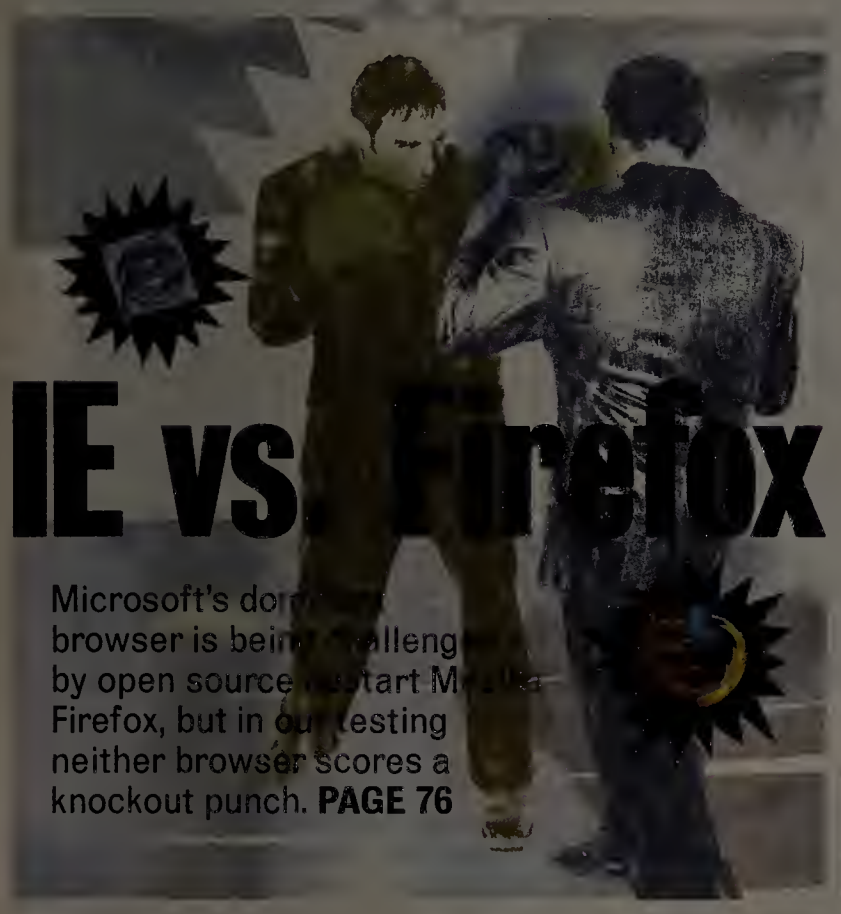
Piecing together the next-generation IT architecture

plus, plus more. Supplement begins after page 30.

NetworkWorld

The leader in network knowledge ■ www.nwfusion.com

March 21, 2005 ■ Volume 22, Number 11



IE vs. Firefox

Microsoft's dominant browser is being challenged by open source upstart Mozilla Firefox, but in our testing neither browser scores a knockout punch. **PAGE 76**

Nortel's 10G switch deals Cisco a blow

■ **BY PHIL HOCHMUTH**

Nortel's long-anticipated, next-generation 10G Ethernet switches will be the centerpiece of a $6.2 million converged network the vendor is building for the city of San Jose -- a contract Nortel won last week.

A botched $8 million Cisco deal with the city ended in scandal last year, which was particularly embarrassing for Cisco — especially because it is headquartered there.

San Jose will install four Nortel Ethernet Routing Switch 8600s, based on the vendor's latest 10G architecture, slated to be announced next month. Based on its former Passport line, the new technology brings Nortel's high-end switch up to speed with 10G gear from rivals 3Com, Cisco, Extreme Networks, Force10 and Foundry Networks, observers say.

The deal with San Jose also is a coup for Nortel, as it won a re-bidding process for the project after the city canceled an agreement with Cisco when an investigation turned up irregularities in how it was awarded. In that deal, an independent auditor found that Cisco and city IT staff had inappropriate contact during the RFP process. As a result, San Jose CIO Wandzia Grycz resigned in August.

The core of the San Jose City Hall building's LAN will be built on Nortel's forthcoming Ethernet Routing Switch 8600 Version 4.0. Formerly the Passport 8600, Nortel is re-branding the product as part of the Ethernet Routing Switch line, a family that also

See Nortel, page 89

Forum airs wireless worries

■ **BY JIM DUFFY**

NEW ORLEANS — Large corporations face a number of daunting issues — from device administration to service-level consistency — as they look to increasingly mobilize their workforces, according to experts at last week's CTIA Wireless 2005 conference.

Companies are adopting wireless technologies in greater numbers as they try to stay connected to workers who are in the office less and in front of customers more.

Moreover, IT managers need to monitor, manage and secure these devices as if they were hardwired to a desktop within the company. And they must do so while keeping the number of mobile devices and the associated expense to a minimum as wireless applications, standards and technologies continue to evolve.

"Who carries one device and has it do everything they desire?" Sprint Executive Vice President Kathy Walker asked rhetorically during a conference session on the industry migration to 3G technologies.

Walker's query reflects the hurdles and questions facing the industry as it attempts to take enterprise mobility beyond just wireless voice and e-mail, two applications that typically require at least two devices. One mobile device per user is hard enough to manage, let alone two. Add to that the tendency of mobile workers to purchase their own handsets and wireless services for business and personal use, and the management task for IT can take on increasing complexity.

"The biggest issue is policy and

See CTIA, page 88

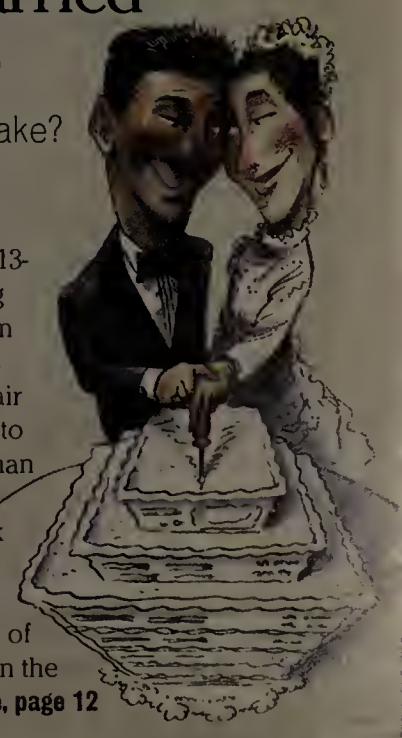
NEWSPAPER ■ $5.00

A Wider Net

Of love and pagers: The life of married network pros

Who will feed the pet snake?

■ **BY CARA GARRETSON**



For Doug and Ellen Chick's 13-year-old daughter, spending an evening in a server room doing homework on the floor is not unusual. As the child of a pair of network managers, she's had to come along for the ride more than once when an emergency calls one of her parents back to work after hours.

"My daughter has written her name on the underside of some of the most expensive equipment in the

See Love, page 12

Charting a Web Course

Redline Networks helps medical records management firm ChartOne cure network pains and boost the business case for its Web-enabled ERP apps.

Redline Networks' E|X 3250 gave Henry Svendblad the performance he was after for ChartOne's Web applications.

Photograph by Robert Houser

NO IT EXECUTIVE LOOKS FORWARD TO ASKING upper management to spend $200,000 on a major system upgrade. But Henry Svendblad, director of IT at ChartOne, Inc., felt he had little choice.

ChartOne, based in San Jose, California, sells technology and services that help health care institutions easily and cost-effectively access and manage patient records. To better serve its customers, which represent 20% of hospitals in the U.S., and to ease the burden on its own IT staff, the company wanted to migrate its ERP applications to the Web.

Like many companies transitioning to Web-based applications, ChartOne hit performance snags that no amount of application tuning and new hardware could cure. Only after two years of trial and error did ChartOne find a cure in Redline Networks, which makes a family of appliances that deliver a broad set of capabilities to ease the network burdens and boost the business case for Web-enabled applications. With Redline's E|X 3250 enterprise application processor handling I/O processing, connection management, compression, load balancing and SSL processing, ChartOne customers and internal users are now experiencing the performance they require — and the company's IT group is realizing the administrative benefits that Web-enabled applications can bring.

ON THE WEB TRAIL

ChartOne's odyssey began in July of 2001, when the company began migrating its homegrown client/server enterprise applications to Peoplesoft 8, a Web-based ERP suite. "We were expecting growth of 20% to 30% a year, and we felt we needed a big ERP system," Svendblad says. In addition, thin, standardized browsers would require far less IT support than fat, homegrown clients.

If ChartOne was going to offer Web-based patient records management services, Svendblad also felt the company "should eat our own dog food" and use a Web-based application platform internally.

Webification proved to have its challenges, however. As more application modules and users moved onto the new infrastructure, response times slowed to a crawl. Employees at the company's 10 remote offices sometimes spent hours waiting for tickler screens that had taken minutes to display under the old client/server system. The 10- to 15-person offices had plenty of bandwidth, IT staffers knew: In anticipation of the migration to Peoplesoft 8, they'd deployed T1 links to each site.

Users on the corporate LAN were also having difficulties. By far, the worst off was the accounts receivable department, which processes more than 300,000 transactions per month. Productivity had dropped by 20% because of response time degradation. "During peak usage periods, it was taking people minutes to go from screen to screen," Svendblad says.

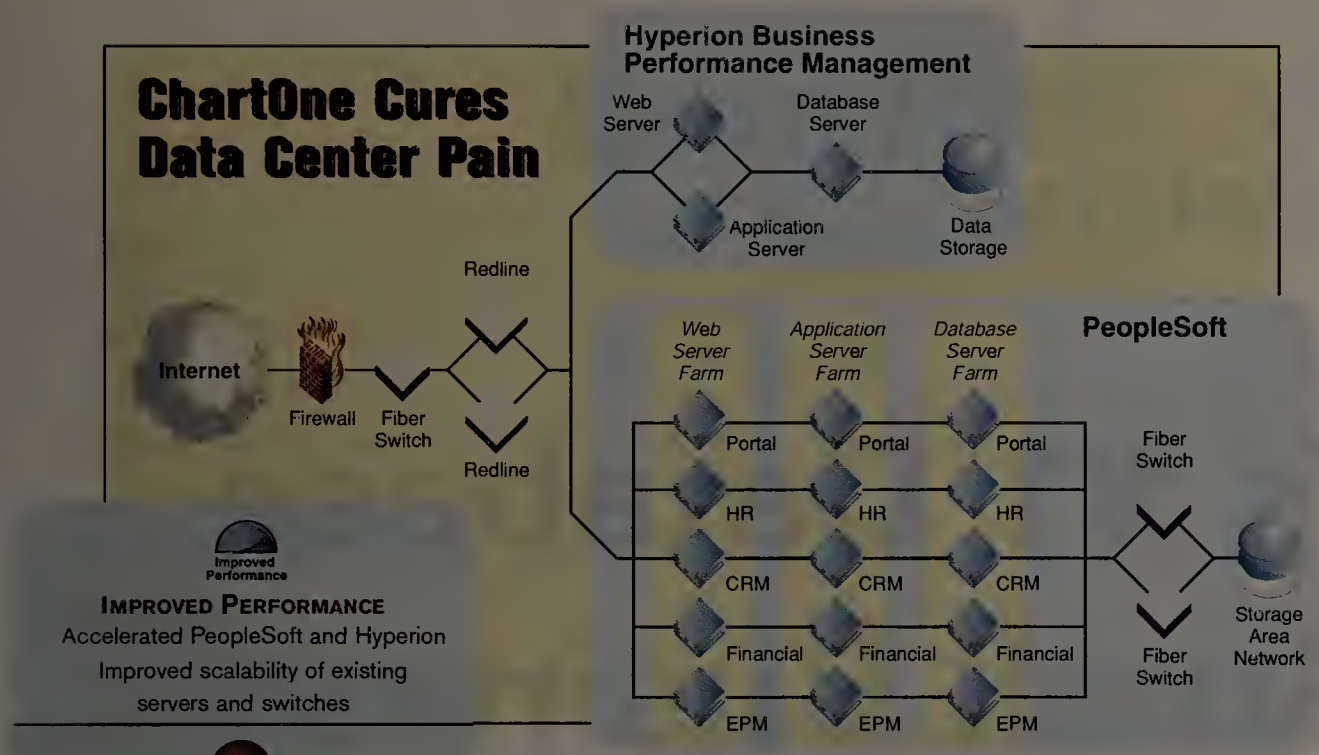
ChartOne's Challenges

- Web-enabled enterprise applications were overloading servers.
- Server processors were at 80% to 90% utilization levels during peak traffic periods.
- Slow response time over corporate LAN was hurting user productivity.
- Remote users waited hours for screen downloads.

The Redline Networks Cure

- Average server CPU utilization during peak usage now between 10% and 15%.
- Response time returned to desirable levels for local and remote users.
- Remote sites no longer need terminal servers.
- Bandwidth consumption decreased approximately 70%.
- Savings of $200,000 by avoiding major hardware upgrades.

Produced by NetworkWorld CUSTOM MEDIA SOLUTIONS



IN SEARCH OF A CURE

As user complaints mounted, the IT staff began looking for remedies. PeopleSoft and Oracle — ChartOne's application vendors — initially suggested fine-tuning their applications. "With a thin Web client, ERP systems involve complex querying in the background," Svendblad explains.

When tweaking back-end software produced little improvement, ChartOne tried upgrading its server hardware. It deployed another Sun 420R application server and storage box, then migrated the main financial server from a 420R to a more powerful SunFire server. "Performance improved slightly, but we were still looking at CPU usage in the high 80% to 90% range during peak processing time," Svendblad says. "And our phones were still ringing off the hook."

Pressed for answers, ChartOne even took the radical step of supplying remote offices and home workers with terminal servers. While that substantially improved response time, maintaining the devices offsite was a major burden on the IT support staff. "It was like we'd gone back to a client/server setup," Svendblad says, noting the setup also strained budgets and IT resources.

Meanwhile, Web and application servers were still maxing out during peak usage periods. A major upgrade seemed inevitable. "It looked like we needed a new [BEA Systems] WebLogic server, a new database server and a third server for finance," Svendblad says. His team priced out three SunFire servers on the second-hand market at about $50,000 apiece. He also budgeted $50,000 for a LAN upgrade, bringing the total budget hit to $200,000, which Svendblad calls a conservative estimate.

ONE VERY BRIEF PILOT

Just as he was about to swallow that bitter pill, a former colleague told Svendblad about Redline Networks in Campbell, Calif., and its family of appliances that help enterprises manage the network impact of Web-enabled applications and improve their business case.

In the summer of 2003, ChartOne deployed Redline's E|X 3250 enterprise application processor in front of its WebLogic servers. The Redline device took over complex scheduling of TCP requests and connection management chores for as many as 150 users, saving the Web servers' CPU and memory resources for other activities like page generation. The E|X also performed data compression to speed up server response and conserve bandwidth.

Svendblad's group started out with a pilot test within the accounts receivable group, which took the biggest performance hit after moving to Peoplesoft 8. Setting up users was simple and transparent, Svendblad reports: "I just changed the local DNS setting, and when users clicked on the PeopleSoft icon, they were routed through the Redline box. We didn't have to change anything on our existing architecture, or on the WebLogic or PeopleSoft servers."

User response was fast and dramatic. "People were asking us if we'd put some magic juice in their system," Svendblad reports. When word spread, end users not involved in the pilot "were pounding on our door saying, 'Whatever you did for her, do for me!'" It may have been the shortest pilot on record: A day after the test started, the company routed all the other users through the Redline box.

TALLYING THE BENEFITS

Once the bulk of users was online, the benefits of the Redline device really began to kick in, Svendblad reports. Average CPU consumption during peak processing time plummeted from 80% or more to less than 15%. Bandwidth consumption decreased approximately 70%.

The E|X 3250 now handles SSL encryption, as well. "We have security without burdening our servers with managing certificates or with SSL," Svendblad says. The company also saves money on SSL certificates, since it needs only one for the Redline box instead of one for each server.

Over the past year, ChartOne brought its customer relationship management, HR and Hyperion Business Performance Management applications behind the Redline box. Most recently, the company added its View Manager: Chart Management Suite of ASP offerings to the set of applications front-ended by the E|X platform.

> After ChartOne installed the Redline Networks E|X 3250, user response was dramatically faster. "People were asking us if we'd put some magic juice in their system," says Henry Svendblad, director of IT.

ChartOne's hundred-odd remote and mobile users have completely eliminated their terminal servers and use a standard Web browser to access all applications, via the E|X 3250. "The user experience is improved, and our support costs are lower," Svendblad says.

The bottom line: ChartOne successfully implemented a Web-enabled ERP platform with a "single box solution" that addresses critical Web tier issues while dramatically improving the business case by increasing user productivity and avoiding costly hardware upgrades. End users now experience the same response time levels and productivity they had with customized fat clients — but IT no longer has the support burden. Says Svendblad: "I think that's pretty impressive."

LEARN MORE ABOUT REDLINE NETWORKS ONLINE

Read what leading analysts and other customers say about Redline Networks at our new InfoCenter,or call us at:

1.877.550.6420

Visit: www.redlinenetworks.com/infocenter

Sponsored by

REDLINE NETWORKS

Oracle Database

World's #1 Database Now For Small Business

Easy to use. Easy to manage. Easy to buy at Dell.
Only $149 per user.

ORACLE®

dell.com/database
or call 1.888.889.3982

Terms, conditions and limitations apply. Pricing, specifications, availability and terms of offers may change without notice. Taxes, fees and shipping charges extra, vary and are not subject to discount. U.S. Dell Small Business new purchases only. Dell cannot be responsible for pricing or other errors. Oracle Database Standard Edition One is available with Named User Plus licensing at $149 per user with a minimum of five users or $4995 per processor. Licensing of Oracle Standard Edition One is permitted only on servers that have a maximum capacity of 2 CPUs per server.
For more information, visit oracle.com/standardedition

Copyright © 2004, Oracle. All rights reserved. Oracle is a registered trademark of Orecle Corporation and/or its effiliates. Other names may be trademarks of their respective owners.

NetworkWorld 3/21

News

- **8 Compliance** pressures still mounting.
- **10 Akamai** snaps up **Speedera.**
- **10 AT&T/Treasury deal** in doubt.
- **12** Web services aimed at building **SOAs.**
- **13 Public schools** have hands full with student hackers.
- **14 New IETF chief:** Our work's still cool.
- **16** Stage set for **WLAN standard** compromise.
- **88 Start-up** joins growing field that handles unstructured data.
- **89 Zultys** launches new IP phones.

Net Infrastructure

- **17** CipherTrust bolsters compliance.
- **17** Start-up to manage Exchange systems.
- **18** Symantec evaluates threat potential.
- **19** SAML 2.0 gets standards stamp.
- **20 Special Focus:** Extreme and Foundry keep on ticking.

Enterprise Computing

- **23** Grid technology aids hospital's diagnostics.
- **24 Dave Kearns:** Microsoft getting Active Directory right.

Application Services

- **27** Offsite security complicates compliance.
- **27** Microsoft rolls out business application plan.
- **28 Scott Bradner:** The NSA: Just doing its job.

Service Providers

- **63** Sprint tailors wireless data services for business users.
- **63** IETF launches emergency communications effort.
- **64 Johna Till Johnson:** Ebbers verdict a comeuppance, not *schadenfreude.*

Net.Worker

- **67** MIMO products boost 802.11g nets.

Technology Update

- **69** RFID readers route tag traffic.
- **69 Steve Blass:** Ask Dr. Internet.
- **70 Mark Gibbs:** Back that thang up — some more!
- **70 Keith Shaw:** CTIA highlights more than cell phones.

Opinions

- **72 On Technology:** Keep this survey for future use.
- **73 Ken Presti:** Nortel's turnaround chief takes aim.
- **73 Thomas Nolle:** What else don't we know about VoIP?
- **90 BackSpin:** SBC makes DSL, er, exciting.
- **90 'Net Buzz:** Pair of university researchers say Metcalfe's Law . . . ain't.

Management Strategies

- **81** Adapting to automation: Technology threatens to eliminate many of today's network administration positions, although industry watchers predict more strategic IT jobs to evolve.

■ **CONTACT US** Network World, 118 Turnpike Road, Southborough, MA 01772; **Phone:** (508) 460-3333; **Fax:** (508) 490-6438; **E-mail:** nwnews@ nww.com; **STAFF:** See the masthead on page 14 for more contact information. **REPRINTS:** (717) 399-1900

SUBSCRIPTIONS/CHANGE OF ADDRESS: Phone: (508) 490-6444; Fax: (508) 490-6400; E-mail: nwcirc@nww.com; URL: www.subscribenw.com

Features

Face-Off

Is Layer 5 the best place to attack WAN optimization? Andrew Foss of Swan Labs says yes, but Jef Graham of Peribit Networks says no. **Page 71.**

Presence simmers on back burner:

Presence technology holds great promise, but corporations are taking it slow when it comes to rolling out presence-based applications. **Page 74.**

Should IE stay or should IE go?

CLEAR CHOICE TEST

Some experts recommend that users replace security-challenged Internet Explorer with the Mozilla Foundation's open source browser Firefox. But our testing indicates that it's a more complicated decision than you might think. **Page 76.**

Online: www.nwfusion.com

Breaking News

Go online for breaking news every day. **DocFinder: 6342**

Available only on Fusion

Network World Renovator Award: Call for Entries

Have you overhauled your network and realized a substantial return on the investment, discovered a significant new business opportunity or found a creative way to leverage technology? If so, get in the running for *Network World's* new Renovator Award, the top winners of which will be honored at a celebration in Las Vegas during NetWorld+Interop May 3-5. **DocFinder: 6093**

Network World Radio: Career building

Career-building advice is always useful, particularly in an age when people change jobs every couple of years. Matt Moran, author of *The IT Career Builder's Toolkit* from Cisco Press, joins to talk about what makes a well-rounded IT employee, one upon whom potential employers will look favorably.
DocFinder: 6345

This week at *Network Life*: The Expert's Guide to the Connected Home

Every day, *Network Life* offers everything you need to know to keep your — and your family's and friends' — home network humming. Get the latest news, opinions, reviews, how-tos and more. **DocFinder: 4838**

Wireless LAN Buyer's Guide

Get the latest information on WLAN gear, including client devices and 802.11a/b/g access points, in our just-updated Buyer's Guide. **DocFinder: 6346**

Seminars and Events

WANs: Optimizing your network now

A new Technology Tour Event and Expo packed with immediate-impact ideas, information and strategies to help you optimize the business applications necessary to your company's success. Find out how you can qualify to attend free. **DocFinder: 6352**

Online help and advice

Nutter's Help Desk

How to deploy VoIP gateways

Help Desk guru Ron Nutter helps a reader weigh his options on where to locate VoIP-to-analog gateways. **DocFinder: 6347**

Gearblog

Where's our spam gone?

Mark Gibbs writes: "Today is March 15, and after more than a year of averaging between 3,000 and 4,000 spams per day, the daily average appears to be falling!" Find out why. **DocFinder: 6348**

Telework Beat

Gate-3 Workclub goes under

Net.Worker Managing Editor Toni Kistner looks at lessons learned from the now-shuttered Gate-3 Workclub, a third alternative to working at home or in the office. **DocFinder: 6349**

Home LAN Adventures

Building a media center, Part 4

With the kinks worked out, columnist Keith Shaw says his home-built media center shines.
DocFinder: 6350

Small-Business Tech

Getting out from under Outlook, Part 1

Columnist James Gaskin shows you how assessing your options and determining your needs can show you whether you're a candidate to move off Outlook and Outlook Express. **DocFinder: 6351**

Free e-mail newsletters

Sign up for any of more than 50 newsletters on key network topics.
DocFinder: 6343

What is DocFinder?

We've made it easy to access articles and resources online. Simply enter the four-digit DocFinder number in the search box on the home page, and you'll jump directly to the requested information.

News Bits

Qwest ups bid for MCI

■ Qwest has increased its offer to acquire MCI, in an attempt to derail last month's merger agreement between MCI and Verizon. Qwest now is offering to pay about $26 in cash and stock for each share of MCI, up from its previous offer of $24.60 per share. MCI's board will review the new proposal and respond by the close of business on March 28, it said in a statement. Verizon announced Feb. 14 that it had hammered out an agreement to buy MCI in a deal valued at $6.7 billion. Soon after that deal was announced, Qwest said that it would revise its previous offer. Now MCI has received a revised offer from Qwest of $10.50 in cash and $15.50 in Qwest shares for each share of MCI. The Jan. 31 announcement that SBC plans to acquire AT&T in a deal worth $16 billion triggered the latest round of merger activity among telecom companies.

SEC levels fraud complaint against former Qwest CEO

■ After a series of legal actions against former executives of Qwest for alleged financial fraud, the Securities and Exchange Commission finally worked its way to the top of the executive ladder. It charged former Qwest CEO and Co-Chairman Joseph Nacchio last week with fraud and other securities-law violations. The SEC charges against Nacchio came within hours of a jury convicting another high-profile ex-CEO defendant, WorldCom's Bernard Ebbers, on all charges leveled against him in connection with WorldCom's $11 billion accounting fraud. The SEC's charges are civil, not criminal, but the agency generally conducts its investigations in tandem with the Department of Justice, which has the authority to bring criminal charges. From 1999 to 2002, Qwest engaged in a complex scheme to improperly record more than $3 billion in revenue and exclude $17.3 million in expenses, according to the SEC. Nacchio's attorney, Charles Stillman, said Nacchio cooperated with the SEC's investigation and that he maintains his innocence.

Senator files anti-phishing bill

■ Sen. Patrick Leahy (D-Vt.) recently introduced a bill to the Senate that attaches fines and prison sentences to scammers caught phishing. The Anti-Phishing Act of 2005, which is similar to the bill Leahy introduced in 2004 that never came up for a vote, slaps phishers with up to five years in prison and fines as high as $250,000. In addition to outlawing phishing, where scammers send e-mails designed to extract personal or financial information from recipients, the 2005 version of the bill also covers pharming. That practice redirects a PC user's browser to a fraudulent Web site asking for sensitive information. While last year's bill was introduced mainly to raise awareness of these scams, a spokesman for Leahy said the senator hopes the 2005 version will pass "sooner rather than later."

COMPENDIUM

Reverse engineering

Google came under some fire for proposing an add-on to its browser toolbar that would do things such as auto-link addresses on Web pages to maps. Mark Pilgrim has done the reverse, coming up with a Firefox plug-in that removes ads from most Google pages and links news queries to non-Google news sites. ***Read more at www.nwfusion.com, DocFinder: 6343.***

TheGoodTheBadTheUgly

Metcalfe medals. Ethernet might be old, but it's not forgotten. Inventing the ubiquitous network technology in the 1970s scored Robert Metcalfe a National Medal of Technology, awarded by President Bush last Monday. (See related story, page 90.)

McOutsourcing. We sympathize with IT folks losing their jobs as companies seeking to operate more efficiently outsource call center and other jobs to people overseas. But news out of McDonald's last week suggests that the trend really might be going too far. The restaurant chain's CEO, Jim Skinner, told investors: "If you're [at a drive-through] in L.A. . . . and you hear a person with a North Dakota accent taking your order, you'll know what we're up to." ➤

BRIAN GAIDRY

Don't mess with 911. A Louisiana man sent a malicious program using e-mail that caused Microsoft WebTV customers to call the 911 emergency service without their knowledge, and now he is paying the price. The man is going to jail for six months after pleading guilty to intentionally causing damage to computers and causing a threat to public safety, according to a statement released by the U.S. Attorney's Office for the Northern District of California.

Bush names Martin new FCC chairman

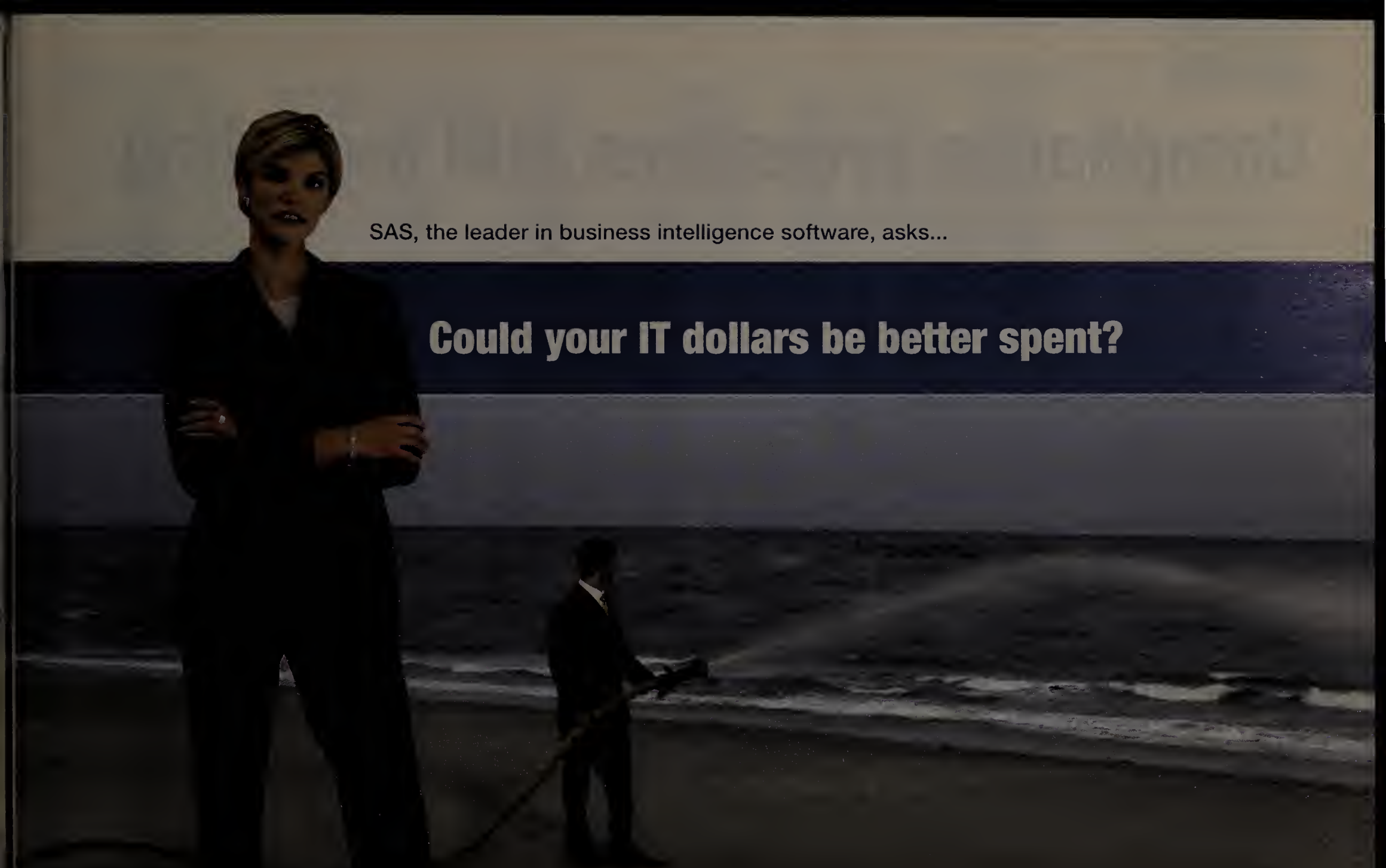
■ President Bush last week named FCC Commissioner Kevin Martin to replace outgoing Chairman Michael Powell as head of the regulatory body. Martin, a member of the FCC since 2001, also served as a special assistant to Bush and was a lawyer with the Bush 2000 campaign. Martin's appointment was largely lauded by the telecom industry. Announcements regarding a commissioner replacement for Martin have not been made. While Bush's appointment of Martin to the head of the FCC doesn't need approval, the White House's candidate for commissioner will require a nod from the Senate before being installed.

Group urges increase in federal R&D

■ The U.S. is in danger of losing its technological edge unless its government increases funding for R&D and reforms the nation's education system, members of the Semiconductor Industry Association said last week. SIA members, including Intel CEO Craig Barrett, called for a yearly 7% increase in the National Science Foundation's research budget, and increases in federal funding of microelectronics and nanomanufacturing programs. They also called for a math and science program in the No Child Left Behind Act. Without a renewed national focus on R&D and education, the semiconductor industry could run into technology and economic roadblocks by 2020, SIA members said at a press conference. Barrett called R&D spending and educated workers the foundations for innovation and creativity in the U.S. But federal government spending on R&D — which funds university-based research in the U.S. — has been flat for about 25 years, SIA members said. The U.S. ranks near the bottom of industrialized nations in science and math education, based on test scores, and the number of U.S. residents applying for doctorate-level degrees is shrinking, Barrett said.

"From a people standpoint, we're not doing a particularly good job," Barrett said. "I don't have particular concerns in the near term about our industry, but I have great concerns about our industry 10 to 15 to 20 years out."

SAS, the leader in business intelligence software, asks...



Could your IT dollars be better spent?

SERVICE LEVEL MANAGEMENT

RESOURCE MANAGEMENT

CHARGE MANAGEMENT

VALUE MANAGEMENT

No business wants to believe it's wasting precious IT dollars. So if executives and co-workers grumble about IT service, and you're convinced those services could be put to better use, let SAS help. With SAS® IT Management solutions, you can measure, manage, understand and communicate the quality of every IT service more accurately. You'll know precisely how your business is using IT resources. Ensure maximum performance and response times. Predict strategic and financial trends. And clearly visualize the value of IT from business, revenue and profit perspectives. Visit our Web site to learn more and read our free white paper, *Align IT with Business and Budget Strategies*. Or call us toll free **1 866 731 1364**.

www.sas.com/spent

Author Nicholas Carr and top business influencers join in a lively discussion about his controversial book, Does IT Matter?
Check out our Web site for more on this informative, on-demand Web seminar.

SAS 9

The Power to Know. | sas®

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration. Other brand and product names are trademarks of their respective companies. © 2005 SAS Institute Inc. All rights reserved 322390

Compliance pressures still mounting

Regulatory requirements, mainly Sarbanes-Oxley, continue to squeeze IT budgets and staff.

■ BY DENISE DUBIE AND ANN BEDNARZ

The tab for regulatory compliance continues to climb — and along with it, demand for IT projects to bolster security, storage and reporting capabilities.

U.S. companies will spend $15.5 billion on compliance-related activities this year, according to research published last week by AMR Research. A large chunk of the spending is designated for public companies' projects related to the Sarbanes-Oxley (SOX) Act of 2002. SOX spending will grow 11% from $5.5 billion last year to $6.1 billion this year, AMR says. Other budget-consuming initiatives include compliance with the Health Insurance Portability and Accountability Act (HIPAA), Food and Drug Administration regulations, and the Basel II international banking accord.

In particular, SOX has put a spotlight on compliance initiatives since it affects a broader swath of companies than some of the industry- or geographic-specific regulations, says John Hagerty, vice president of research at AMR Research. Additionally, it's getting budget priority over other regulatory projects because its deadlines are imminent. "Those with the shortest deadlines move to the top of the queue," he says.

Passed in the wake of accounting scandals at companies such as Enron and WorldCom, SOX is designed to deter fraud and add transparency to public companies' financial reporting procedures. Among the more onerous of the legislation's requirements is Section 404, which calls for companies and their auditors to formally attest to the existence and adequateness of internal controls over financial reporting systems.

Establishing, testing and documenting such controls is a time-consuming effort that not only has financial departments scrambling but involves nearly every aspect of IT.

The toughest part of SOX compliance is the scrutiny it places on the IT department, says James Olson, CIO at Waterbury Hospital in Connecticut. SOX has increased the number and comprehensiveness of IT-related audits, he says. "It used to be that a 100-watt bulb would be turned toward IS once a year. Now we have a searchlight looking at us."

Prior to the legislation, auditors examined the hospital's patient accounting system. Today, audits extend to multiple applications, including accounting, payroll, materials management and decision support systems.

Auditors today look not only at backup, data center security and password administration but also division of labor within the department, Olson says. "They have increased what they are auditing and [now look into] the formality of the policies, procedures and processes supporting the department," he says.

What makes SOX tough is that there's no one-size-fits-all checklist for compliance, adds James Kritcher, vice president of IT at White Electronic Designs. "From an IT perspective, the actions that a company will need to take depend on what is discovered in the internal controls inspection. IT leaders need to work closely with the Sarbanes-Oxley auditors to make sure that they know what their companies' weaknesses are."

When it comes to choosing technology to help with Section 404 compliance, purchases run the gamut from security and document management to collaboration and performance management products. There's no shortage of vendors offering SOX compliance assistance.

For example, OpenService this week is expected to release new versions of its flagship Security Threat Manager software, as well as Security Log Manager, an add-on monitoring application that alerts security managers to events that don't comply with predefined SOX policies.

Last week, SAP announced a deal with compliance specialist Virsa Systems to offer its Compliance Calibrator software to SAP users to help keep tabs on ERP system controls and avoid segregation-of-duties conflicts among end users.

Getting help

To automate manual processes, Waterbury Hospital has purchased configuration control software for patching its servers, password control software and other technology, Olson says.

White Electronic Designs uses automated configuration management tools from Ecora and Tripwire to automate some of its SOX requirements, Kritcher says. The Phoenix company uses the tools to document baseline device configurations and detect unauthorized infrastructure changes, he says. "Without these types of tools, compliance would be much more difficult."

Even with the tools, the burden of SOX is palpable. "A great deal of IT time over the past year has been spent on Sarbanes-Oxley compliance activities," Kritcher says. "We had to defer a couple of planned, funded projects to divert staff resources to the compliance effort. The current year is looking much the same."

One of the aspects of SOX that has surprised companies is that it's an ongoing effort, Hagerty says. "People thought it would be a Y2K-like effort, but it's not. Companies have to deal with SOX requirements perpetually."

The ongoing nature of SOX compliance is disruptive and costly, Olson says. "The auditors will always find yet one more aspect that needs doing," he says.

But there also are advantages for IT to SOX regulations, which can provide an impetus for companies to formalize their documentation and process controls. Many of the practices SOX has necessitated are good management practices, Olson says. "It is just we always gave them lower priority than our day-to-day stuff so implementation dragged," he says. "Now we have no alternative."

Mike Levinson, IT capacity planning and change manager at Hannaford Bros., a supermarket retailer in Portland, Maine, agrees. Levinson says SOX compliance helped him get management to approve the process-oriented approach he prefers to take. A former IBM systems administrator, Levinson always wanted to instill change management processes at the supermarket chain before SOX auditors hit the scene.

"Sarbanes-Oxley helped us get processes in place that probably should have been in place," he says.

Levinson says an audit of Hannaford's IT shop showed the company could improve its change management processes and its security controls such as defining separation of duties and establishing consistent policies across system platforms.

Levinson notes security policies on Windows, Unix, Linux and mainframe servers — all of which Hannaford has — differ and SOX will require the IT department to define consistent rules across the platforms. Also, SOX security policies, such as incident response, need to be clearly stated to avoid any ad hoc firefighting when, say, a virus breaks out.

Levinson estimates that his IT team spends about 60% of its time fixing problems, which take priority over long-term IT projects. Now with SOX compliance on their list of things to do as well, he says he can't "accurately predict how many resources we will have for IT projects," which means they could potentially miss scheduled deadlines.

Because Hannaford is owned by the Belgium-based Delhaize Group, the company has another year to get compliant with Section 404. The Securities and Exchange Commission this month granted small and midsize public companies with a market capitalization less than $75 million, as well as international companies, a one-year reprieve until July 15, 2006.

Large public companies with a market capitalization of at least $75 million — with some exceptions — must begin including internal control reports required by Section 404 in annual reports filed for their first fiscal year ending on or after Nov. 15, 2004.

Looking ahead, AMR's Hagerty says companies will become more strategic about addressing SOX. Efforts this year will shift away from manual processes and toward automating compliance, he says. "Fixes are heavily manual today, but that can't go on indefinitely or it would pose a real hindrance to business."

Kritcher says he sees an opportunity to shed some compliance costs and free up IT resources "by implementing systems and processes that simplify the compliance monitoring and audit process." As companies put compliance controls in place it makes sense to look for process re-engineering opportunities, he says.

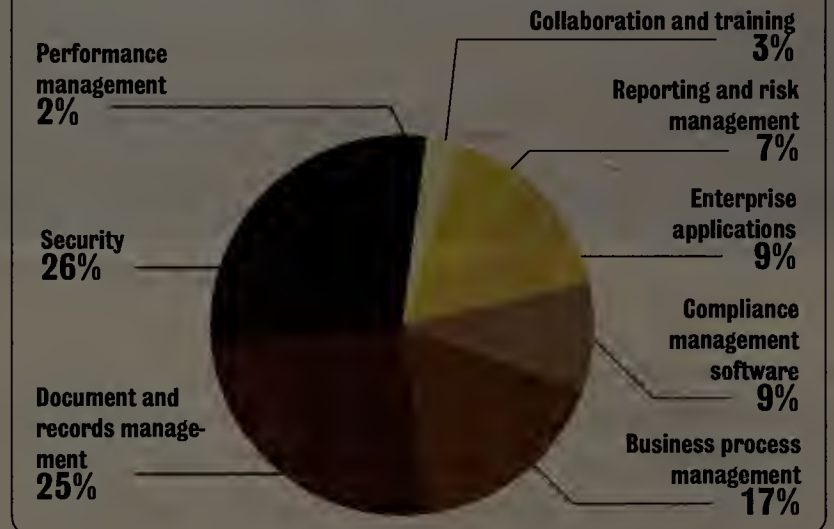
Shifting SOX budgets from headcount-related costs to technology purchases reflect shifting mind-sets, Hagerty says.

Whereas companies spent about $1.1 billion in 2004 on SOX-related technology, this year they will spend $1.7 billion, he says. "People are spending more in '05 than '04 because they realize they have to automate a lot of the stuff they did by brute force last year."

Next up is finding ways to use technology to remediate any compliance shortcomings. By the end of 2005, companies will begin to deploy technology not only to automate processes and identify gaps, but also to help automatically close up any gaps that appear, Hagerty says. ■

SOX technology priorities

Security products top the list of technologies that companies plan to purchase to aid in Sarbanes-Oxley compliance, according to a survey by AMR Research of 95 people.



■ Read how offsite security causes problems with Sarbanes-Oxley compliance. PAGE 27.

RECLAIM YOUR EMAIL

Visit us at Info Sec.
Booth #813
Orlando

Spam and virus protection at an affordable price.

- No per user license fees
- Prices starting at $1399
- Powerful, enterprise-class solution

Barracuda Spam Firewall

BARRACUDA NETWORKS

Order a free evaluation unit at
www.barracudanetworks.com

POWERFUL EASY TO USE AFFORDABLE

Aggressive Reseller Program
Get more info by visiting www.barracudanetworks.com/ptnr
or by calling 1-888-ANTI-SPAM or +408-342-5400

Buyout ends Akamai, Speedera feud

■ BY JENNIFER MEARS

The news last week that Akamai Technologies had acquired Speedera Networks confirmed two things: The deal will end the companies' bitter rivalry and the content delivery market has matured out of its turbulent adolescence.

The acquisition, still subject to regulatory approval, is aimed at creating a global content delivery network (CDN) powerhouse that can better compete with emerging content and application delivery services from bigger players such as AT&T and Savvis Communications, (which through a series of acquisitions owns CDN firm Digital Island), Akamai executives say. In addition, it puts an end to drawn-out legal squabbling between the two firms since all litigation is stayed as a result of the merger agreement.

"By the standards of business actions, it really makes a lot of sense. ... It's a simple, face-value good deal," says Peter Christy, cofounder of NetsEdge Research Group. "But if you read between the lines, there were a bunch of legal actions that were about to reach some serious event. ... There was a call to action, there was a reason this happened now, otherwise the barrel was going to go over the waterfall."

The acquisition appears to be a good deal for Akamai, which eliminates a primary competitor and gains access to some 350 companies, as well as a presence in India. Speedera last fall opened operations in Bangalore, and has 50 of its 125 employees there, says Ajit Gupta, Speedera's president, CEO and founder.

What the deal means to customers is less clear.

Playing nice

After years of battling it out, content delivery specialists Akamai and Speedera are joining forces. A look at the two firms:

	Akamai	Speedera
Year founded	1998, IPO in 1999.	1999, private company.
Number of customers	More than 1,300, including FedEx, Toyota and the Department of Defense.	350, including HP, Lowes and NASA.
Size of overlay network	14,000 edge servers in 1,100 networks in more than 65 countries.	Edge servers with connection to more than 1,000 networks.
Sampling of services	On-demand hosting services, business continuity, site security and dynamic application delivery.	Support for eCommerce, site security, business continuity and distributed application delivery.

"It's good for [the companies]. It's just simple consolidation. It's less good for us customers in that it takes away a competitive option, reducing our leverage," says an Akamai customer who asked not to be named. "Speedera was an important alternative supplier. But that said, in general Akamai has been a good partner to us, and we'll probably see some benefit from their increased size and scale."

"Whether it's good news in a general sense for the CDN market, that's harder to say and a little more doubtful," says Lydia Leong, principal analyst at Gartner. "It's removing a competitor and turning Akamai into even more of a powerhouse than it has been in the past."

That could result in more expensive services overall, Leong points out. While smaller players, including Mirror Image, Netli and Limelight Networks, remain, the bulk of the CDN business has been going to Akamai and Speedera for some time.

On the other hand, taking some of the cutthroat competition out of the market might be a good thing, analysts say.

For years, the CDN market has been mired in legal battles, not the least of which has been the back-and-forth between Akamai and Speedera. The two, which defined the CDN market when they were launched just one year apart in the late 1990s, have been archenemies in and out of the courtroom.

Speedera has billed itself as a lower-cost alternative to Akamai. In 2002, when Akamai initially sued Speedera, claiming the company's CDN services infringed on Akamai patents, Speedera had a promotion running on its Web site in an effort to lure Akamai customers to its service. At that time, Akamai also accused Speedera of unfair competition, and later that year filed a lawsuit accusing Speedera CTO Richard Day of breaking into a protected Akamai database.

"It's almost like the Capulets and Montagues have kissed and made up," says Counse Broders, principal analyst for Internet and managed services at Current Analysis. "They have been such major rivals. . . . But they're getting rid of those pesky lawsuit issues. It lets them focus now on the bigger market and not have to worry about their next court case."

Despite the constant bickering, both companies have had recent success.

In February, Akamai reported what CEO George Conrades termed the best financial results in the company's history, with full-year net income of $34.4 million in 2004, compared with a net loss of $29.3 million the year earlier.

As for Speedera, which became profitable in 2003, it reported revenue for the second quarter of $8.28 million, up by half when compared with the same quarter a year ago. The company says its net income tripled when compared with the second quarter of 2003.

Part of the reason for the revenue growth is that both companies have been rolling out more sophisticated services. For example, Speedera last month introduced FlexComputing to host enterprise applications and accelerate their delivery.

Akamai also is focusing on application acceleration and virtual Web hosting, areas that are becoming increasingly important as businesses put more applications onto the Web. ■

AT&T's Treasury deal in doubt

Federal overseers say bid should be reopened after upholding protests.

■ BY CAROLYN DUFFY MARSAN

The Government Accountability Office last week ruled that the Department of the Treasury should reopen negotiations for a $1 billion telecommunications contract that the agency awarded to AT&T in December.

The GAO sustained five protests filed by other bidders on the Treasury Communications Enterprise (TCE) contract. Broadwing Communications, Level 3 Communications, MCI, Northrup Grumman Information Technology and Qwest Government Services filed the protests. A seventh bidder on the contract — Sprint Communications — did not submit a protest.

"We found there was merit to the protests, and we recommend the agency reopen its negotiations," a GAO official said. "Treasury didn't have discussions with all the bidders, and we're telling them to do that."

The GAO received an administrative report from the Treasury Department and held a hearing on the five protests before making its decision. Because the TCE bids involve trade secrets and proprietary information, the GAO decision was issued under a protective order. However, the GAO official said a redacted version of its findings will be released to the public by this week.

AT&T insists it will overcome the setback.

"We're disappointed in the GAO's decision but we fully intend to compete vigorously to retain this award as the Treasury Department amends it and collects additional information from bidders," said Lou Addeo, president of AT&T Government Solutions in a statement. "We strongly believe we submitted far and away a superior solution to Treasury's networking needs, and we look forward to making our case again to Treasury."

The TCE contract would provide telecommunications services and support to more than 1,000 domestic locations and tens of thousands of agency users in the U.S. and overseas. The Treasury Department includes the Internal Revenue Service, the U.S. Mint and the Comptroller of the Currency among its bureaus.

The TCE contract calls for three base years and seven one-year options, and its value is estimated as high as $1 billion.

AT&T Government Solutions planned to build a secure, high-speed IP VPN to handle Treasury's voice, video and data traffic. AT&T's team for the TCE bid included Accenture, BAE Systems and Lucent.

"We definitely plan to rebid TCE," says Jerry Edgerton, senior vice president of MCI's Government Markets Division. Edgerton says TCE is one of the biggest telecommunications procurements underway in the federal government market, and it is among MCI's top priorities this year. ■

Corrections

■ The story "Offshoring closer to home" (March 14, page 25) should have stated that Wayne Gudbranson is president and CEO at IT research and consulting firm Branham Group.

■ The story "Wyse CEO touts software initiative" (March 14, page 21) should have listed Garnett & Helfrich on second reference as G&H.

Servers
Subscribe to our free newsletter.
DocFinder: 5434 www.nwfusion.com

FEEL THE POWER OF LINUX.

Introducing the IBM eServer™ OpenPower™ system. With this server, you can have it all. Power Architecture™ technology and the Linux® operating system. Outstanding reliability features and 64-bit computing. This is what you've been waiting for. A server specifically enhanced for Linux. It's a purist's dream. It's instant entrée into the Linux movement. And it's an affordable way to adopt Power Architecture technology on demand. Join the movement at **ibm.com**/eserver/pumpup

IBM

eserver®

IBM, eServer, the eServer logo, OpenPower and Power Architecture are trademarks or registered trademarks of International Business Machines Corporation in the United States and/or other countries. Linux is a trademark of Linus Torvalds in the United States, other countries, or both. Other company, product and service names may be trademarks or service marks of others. © 2005 IBM Corporation. All rights reserved.

Vendors target Web services/SOA mix

■ BY JOHN FONTANA

Iona Technologies and Reactivity this week are scheduled to unveil their latest infrastructure technology aimed at helping users build service-oriented architectures.

Iona plans to release Artix 3.0, which adds real-time upgrade features, integration with corporate development tools, failover capabilities and support for emerging Web services standards for transactions.

Separately, Reactivity is set to unveil an appliance it calls SOA Gateway, which is designed to provide security and connection to legacy applications for users deploying Web services in and among corporate data centers. The gateway, for use internally, is being paired with Reactivity's XML Security Gateway, which is designed to run on the edge of corporate networks.

Interest in the concept of SOA has grown over the past year as companies find success with initial Web services projects focused on point-to-point integration. Now they want to fit those Web services into an SOA but find they are missing needed tools and infrastructure, according to experts.

"What users are finding out is that the theory of an SOA is more attractive than the reality," says Shawn Willett, an analyst with Current Analysis. "The nitty-gritty is that you need to accommodate a lot of ways to get at information and ways to pass transactions that are not covered by today's Web services standards. People are realizing that and trying to accommodate that."

Willett says users are finding that the definition of a standard is not clean and tidy, and that simple request and response sorts of services don't substitute for transactional integrity. "It is hard to fit that into Web services the way the standards are written right now," he says. "So users have to be flexible in their definition of service in order to build an SOA."

Iona is trying to provide some of that flexibility with Artix 3.0, which runs within the services and is not installed as a hub in the network. Artix uses plug-ins to legacy transaction platforms and applications that help expose those systems as services with support for a wide range of protocols, transports, data models and security standards. New in Version 3.0 is an extension that lets users upgrade services without having to take them down. Iona also has added support for the Eclipse development environment and Visual Studio .Net so developers can use familiar tools when building new services that incorporate Artix.

"It's like application server clustering without the application server," says Eric Newcomer, CTO for Iona, which competes with Sonic, webMethods and Actional.

The Artix 3.0 is slated to cost $10,000 per CPU.

Reactivity's angle is a set of appliances to boost the performance and secure communications within an SOA, especially in the data center, where SOA Gateway is focused.

"In the data center, you have a higher level of transaction rates so there are larger numbers of interactions that occur, and there is a much higher emphasis on identity and access control," says Andrew Nash, CTO of Reactivity.

SOA Gateway integrates with existing authentication and authorization systems such as those from RSA and Oblix, and acts as an access and policy enforcement point in the network. It also logs each transaction. The gateway includes acceleration technology to speed access control and policy lookups, and supports more than 250 XML and non-XML data formats.

The appliance runs on top of Red Hat Linux and includes Reactivity's XML Operating System. It competes with similar products from Datapower, Sarvega and Forum Systems.

Software and appliances from Iona and Reactivity come on the heels of Vordel's updates earlier this month to its Secure XML Gateway and Director products. Both feature a new XML schema editor that generates an XML schema from a message based on Simple Object Access Protocol. Secure Gateway has been updated with an XPath wizard, which lets users specify what parts of an XML document must be signed and encrypted, and integration with Web access control platforms from RSA.

SOA Gateway costs $65,000. ■

Love

continued from page 1

world," jokes Doug, the 43-year-old director of IS for Katsur Management in Orlando.

That's one of the downsides to being network managers in love — both partners are always on call. This can mean priorities at home take a back seat; the dog doesn't get walked, the school play is missed, an algebra assignment is done behind a server rack.

Life's no easier for Jeff and Andrea Westerinen, a pair of product developers who both work for technology companies. When laundry doesn't get done at the Westerinen household because of crazy travel schedules or long evenings at work, Jeff, a 48-year-old architect at Microsoft, suggests the family just buy new underwear. His wife, Andrea, an architect at Cisco, doesn't react quite as breezily. "When we're really busy, who worries about dinner and the laundry?" asks Andrea, also 48. "That's probably my domain."

It's not that demanding travel and long hours are unique to technology professionals, but Andrea feels this industry puts more pressure on employees than most. "You're expected to be on e-mail, to be accessible, to do your phone calls with India at bizarre times of the day. In the high-technology business, you bring your work home with you," says Andrea, who spends two weeks a month away from the family's home in Seattle at Cisco's San Jose office, in addition to other travel.

When Andrea and Jeff's travel schedules collide, the couple calls in reinforcements. They have flown in family members from other states to take care of their 11-year-old daughter when they're both on the road, and often rely on neighborhood kids to feed their pet snake, tortoise and fish when they're working late and their daughter is staying with a friend.

Most frustrating for her is when travel makes her miss her daughter's concerts. "That's the worst," she says, "when you feel maybe the industry is costing you too much."

Family vacations at Comdex?

The Chicks, who occasionally attend industry conferences together, have been known to bring their daughter to local events, but have stopped short of turning work-related travel into family travel. "I don't think our daughter would be too happy if we announced that this year's family vacation was going to be at Comdex," says Ellen Chick, a network engineer with a network consulting company also in Orlando.

Andrea and Jeff Westerinen call on extended family and neighbors to help with childcare and pet feedings.

Managing home life can be particularly challenging when both partners begin the second part of their workday after dinner. Such is the case for Lakshmi Sailaja, a senior consultant with software development outsourcer Sierra Atlantic, and her husband, Balaji Gangishetty, who is a principal consultant with the same company. The couple met at Sierra Atlantic's Indian office in Hyderabad and two years ago moved to Fremont, Calif., to work for the company's U.S. operations.

Both need to be in contact with the company's Indian office multiple times a week, which because of the time difference means calling overseas at about 10 p.m. "I'm sitting in one room of the house on the phone, and she's sitting in another room on the phone," Gangishetty says.

"Some days you get into calls that go until 12 at night ... you come out of the call, and your mind is still on it for the next half an hour."

The couple has set a few basic rules to keep work from swallowing up their lives: no talking about work over dinner and no working on the weekends.

Allowing for work-related chatter at home can be both good and bad, says Ellen Chick. "There have been times when [Doug] has been telling me about a particularly frustrating encounter with an end user, and I find myself living it and getting frustrated too," she says. "Sometimes it's like, 'I've already lived one day at work, I really don't want to come home and live another one.'"

But it also means partners can vent without having to provide context. "Let's face it, any IT person coming home to a non-IT person is not going to get to have a 30-minute conversation about the new server they just racked," Ellen says.

"It is fantastic to have someone with enough commonality in the type of work I do that she can understand and relate to the situations and problems I encounter at work," echoes Jeff Westerinen about Andrea.

But the Westerinens also know what it means to be too close to their spouse's job; they worked together at IBM, NCR, Intel and Microsoft before Andrea was hired by Cisco.

"Then it was harder to talk about work. It's hard when your spouse likes somebody and you hate them," says Andrea, who has vowed to never work for the same company as her husband again. "It got almost incestuous: You couldn't vent to the other person because they knew the situation."

So after a long day at work, who fixes the home network when it's on the fritz? "Somehow I'm always the one playing IT administrator when things go wrong with the [home] network or computers, which I absolutely hate," Jeff Westerinen says.

Leaving management of the home network to her husband is one of the secrets to limiting arguments, Ellen Chick says. "Having two people manage the same network is like two people cooking the same meal ... in one pot ... in a camper," she says. "I don't mess with it." ■

Juniper Your Net™

For his company's growth to balloon, Bob knew he'd have to initiate a network change... a prickly subject for sure.

NETWORK EXCELLENCE

QUESTION: IS SWITCHING FROM THE STATUS QUO A STICKY SUBJECT INSIDE YOUR ENTERPRISE? READ ON, THEN LEAD AN ENTERPRISE-WIDE CHANGE FOR THE BETTER.

Simply Juniper *your* net and change complex legacy configurations into clean-slate convenience. Our comprehensive solutions deliver unprecedented heights of speed, unbelievable depth of processing, unsurpassed security.

▸ **LEADING THE WAY WITH SECURE, ASSURED NETWORKING, ONLY JUNIPER.**

Security, with assured performance. Juniper's promise, and a unique, industry-altering brand of networking. *Secure & Assured Networking* is application-driven: End-to-end network control, with guaranteed application delivery and performance – network wide. It's ceaseless security assessment: Deep inspection firewalls, Intrusion Detection and Prevention, as well as application-aware remote access SSL VPNs. It's certain performance: Predictability through high-availability and platform stability – all via scalable platforms. Just because users have access doesn't mean they should have the run of your resources – that's *Secure & Assured Networking*.

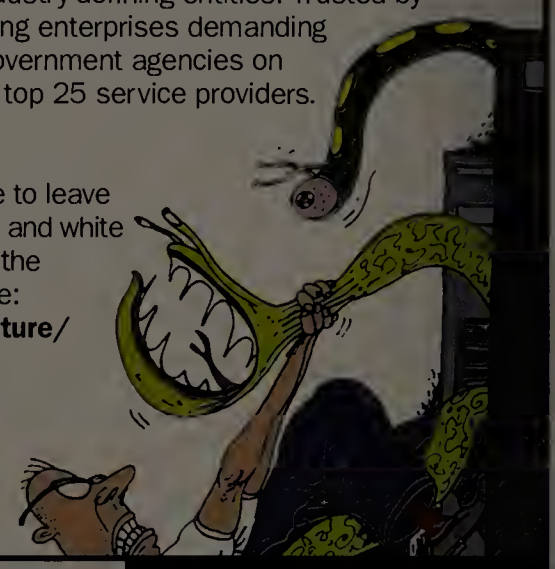
Juniper means security and assurance legacy players can't emulate, only envy. Because it's impossible to bolt onto their antiquated hardware what's built into our innovative software. Juniper architecture creates incredibly scalable solutions, helping eliminate downtime, upgrades and workarounds while improving speed, reliability and performance. That's how a Juniper network thrives in the most demanding conditions, allowing customers to build and run networks in the harshest, most competitive environments – so forge ahead and fear not.

▸ **A LEADER FOR BRAND LEADERS, IT'S JUNIPER.**

Juniper's carrier-class performance, intelligence and security – once available only to SPs – is here for your enterprise. That's why we're the recognized leader, and the preferred brand of mission-critical, industry-defining entities. Trusted by the largest firms on Wall Street, the leading enterprises demanding perfect performance, the most vigilant government agencies on worldwide watch to, count 'em, 25 of the top 25 service providers.

▸ **LEAD THE WAY, WITH JUNIPER.**

Need more help convincing your enterprise to leave the status quo? Get insightful case studies and white papers, clear competitive advantages and the networking news you need. And get it here:
http://www.juniper.net/solutions/literature/



www.**juniper**.net

888-JUNIPER (888-586-4737)

Juniper® NETWORKS

© 2005 Juniper Networks

K-12 schools fight to stymie kid hackers

■ BY ELLEN MESSMER

It's enough to make you long for the days of spitballs in the classroom. When today's K-12 students act up, they increasingly are going high-tech by using the school's network to launch denial-of-service attacks, sending harassing e-mails or breaking into databases to try to change their records.

With public schools now widely equipped with LANs and high-speed Internet access, IT administrators have to cope with students who run amok in many ways. Some infractions, such as attempts to get to pornography sites, might force administrators to temporarily yank a child's network access as punishment. But some types of incidents, such as hacking and e-mail threats, even end up with students being booted out of school or in trouble with the law.

"The main problems start developing around 7th or 8th grade," says Lee Sleeper, technology manager at Bullard Independent School District in Texas, which has 1,650 students who get a password and account to access a multi-Gigabit fiber network and the Internet. Each 8th- to 12th-grader also gets an e-mail account.

The network troublemakers — perhaps 5% of the older students — are often bright but have fallen sway to the notion that network misbehavior, especially hacking, is "cool," Sleeper says. "I'm trying to identify the 'little darlins' who are so creative and get them on my side."

Like most school districts in the country, Bullard uses Web-filtering software to block access to inappropriate Web sites, whether it be pornography, games or hate sites.

Students and parents are asked each year to sign an acceptable-use policy, which states that the student won't wrongfully exploit the network. According to the Department of Education, which last month released statistics about K-12 networks in a report, 83% of schools had such contracts.

The Department of Education notes 48% of public schools also let students access the Internet outside of regular school hours.

But just because the Bullard district's students sign the acceptable-use policy doesn't mean all's quiet on the network front.

Students still try forbidden searches. One case Sleeper is trying to sort out concerns a high school girl who says she didn't try to access porn sites — that someone stole her password. Usually, the punishment would be temporarily disabling the transgressor's account after consulting with teachers and other staff, but stolen password allegations make resolving these incidents far more difficult.

Upping the ante

Network hijinks get worse.

"A neighboring school district had a student who miraculously had no absences," Sleeper says. This prompted suspicion among school staff. It turned out the student appropriated a clerical account and changed the school records. The case led to criminal charges.

Sleeper says schools have to teach responsibility and ethics in technology use and offer the tools of the modern world, but in every generation, there are times when "the whole interest in life is in circumventing the system."

Philip Scrivano, management analyst at the Bakersfield, Calif., Fiscal Crisis & Management Assistance Team (FCMAT), agrees. His organization gets state funding to assist California schools through various troubles, including network-related ones.

"There is the sub-culture of coolness in" inappropriate network behavior, he says. "Kids will play around, especially junior high school boys."

Scrivano says that in his role as adviser, he's seen three students expelled for installing a keylogger on the teacher's PC and changing grades. He's also seen students expelled for breaking into servers. While school staff want to temper justice with mercy, the situation is simply that some troublemakers are spending inordinate amounts of time planning break-ins — sometimes 50 to 100 hours for one attack.

The hard part is making teenagers understand that what they're doing is a crime. Andy Prestage, another management analyst at FCMAT, says children sometimes brag to the media about what they've done — and the outcome is they get arrested. Some serve jail time or get fined. FCMAT itself provides both legal and computer forensics support to California schools.

Taking countermeasures

In the Palm Springs Unified School District in California, which has 22,000 students and 28 sites, students trying to hack into school records caused enough problems that the district installed an intrusion-prevention system from McAfee, says Rick Corl, director of technical services for the school district.

"We had students hacking into our information systems from other school districts," Corl says. Some students also launch DoS attacks on the school's domain name, he says.

In the Bryan County, Ga., system — which has nine schools and 6,000 students who have T-3 access to the Internet — the daily battle that network administrators fight is preventing game and music downloads while striving not to block the passage of educational files by teachers.

But one incident — where a teacher was mailed suggestive and threatening e-mail — forced the IT department to work with Georgia law enforcement and a local ISP to track down the source, says Technology Director Jay Meeks.

The e-mail turned out to be from a student's home computer. Because the child admitted what he did, the school took correctional action, which largely focused on counseling. "But if the child hadn't admitted what he did, it would have been a different outcome," Meeks says.

At the very least, students are punished for violating acceptable-use policies by having their network access yanked. That's getting harder to do since teaching, learning and doing research in American schools is more and more coupled with networks.

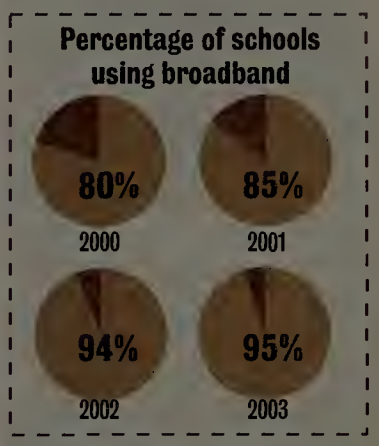
"We've had students' network privileges or computer removed for the school year," says Becki King, technology coordinator for the Northern Community Schools of Tipton County, Ind., which has 1,000 students. "But that makes it harder for them to do their schoolwork."

IT administrators say they don't like being cast in a Big Brother-role on school networks, but the primary focus is on safety.

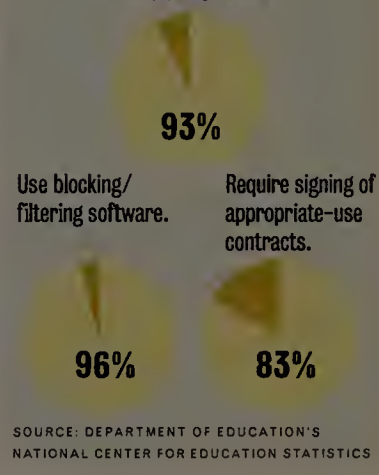
"We worry about a lot of things, including outsiders getting into the network," Sleeper says. The worry about chat-room contacts becoming dangerous to students means that the school district doesn't permit chat and blocks access to it. ■

School safety

With the percentage of schools outfitted with broadband Internet access on the rise . . .



. . . schools are taking steps to ensure safe network usage.



SOURCE: DEPARTMENT OF EDUCATION'S NATIONAL CENTER FOR EDUCATION STATISTICS

NetworkWorld Renovator Award

Have you overhauled your network and realized a substantial ROI, discovered a significant new business opportunity or found a creative way to leverage technology?

If so, get in the running for *Network World's* new Renovator Award, the top winners of which will be honored at a celebration in Las Vegas during the NetWorld+Interop conference, May 3-5.

Entries will be judged by a panel of *Network World* editors, columnists and industry experts. Winners will be presented an award at the celebration and profiled in a subsequent *Network World* story.

Stand up and be counted.

Enter today at **www.nwfusion.com/renovator2005.html, DocFinder: 5951.**

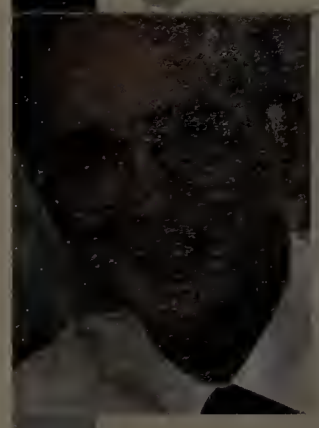
All entries must be received by March 28, 2005.

Judging panel

Bob Brown, Executive News Editor, *Network World*
Daniel Golding, Senior Analyst, Burton Group
John Dix, Editor in Chief, *Network World*
Johna Till Johnson, Founder and CRO at Nemertes Research
Lee Doyle, Group VP, Network Infrastructure, IDC
Jeff Wilson, Principal Analyst, Infonetics
Robert Whiteley, Analyst, Forrester Research

Sponsored by Juniper® NETWORKS

Q A New IETF chief: Our work's still cool



Brian Carpenter, a distinguished engineer with IBM, has taken over as chair of the IETF, the Internet's foremost standards-setting body. Carpenter is the sixth person to chair the IETF since its founding in 1986. Network World *Senior Editor Carolyn Duffy Marsan had an exclusive interview with Carpenter at the group's recent meeting in Minneapolis. Here are excerpts from their conversation:*

What is your role at IBM?

I handle internal coordination regarding the IETF. I'm also working on product development strategy for networking. The IETF chair is a full-time job, but I am keeping a few customer projects. I don't want to be too removed from reality.

What do you hope to accomplish as IETF chair?

My first goal is an internal goal for the IETF, but I would like to get the Internet Engineering Steering Group into a position of steering and not just processing documents. I would like the members of the steering group to get into more strategic issues of where we should be going in the future. Second, I want to improve our liaison relationships with other standards bodies, including the International Telecommunication Union, the Third Generation Partnership Project and the Open Mobile Alliance. I want these relationships to work in both ways.

What is the most important technical work going on in the IETF right now and why?

I still believe that getting IPv6 deployed is very important. I think the people who say we can go on with IPv4 are strategically wrong. Second, I think we have work to do in the security area. There is still more work to be done to have an overall security model. The other important work is [Session Initiation Protocol] and everything that goes with SIP. This is where the liaison issue with the ITU comes up because we'll be using SIP to run regular telecommunications services over the Internet.

What will you do as IETF chair to promote IPv6?

The IETF's main job on IPv6 is done, and it is now shipping in major operating systems. It's now a deployment issue, not a development issue. The IETF needs to keep saying that IPv6 is a strategic technology and that it's ready. There is already strong commitment by the U.S. Department of Defense, China and the 3G [Partnership Project] to IPv6. A small or medium-sized business probably has no urgent need for IPv6. But for the enterprises, sooner or later they will notice that all their operating systems and routers can do IPv6. Then they'll notice that it's not a big capital expense to move to IPv6. But it may be a big deal operationally.

Many IETF working groups are behind schedule. What will you do to encourage them to wrap up their work?

There's no single answer. When you dig into why something is moving slowly, it might be pure sociology as in the working group dynamics or it could be a patent issue or a general technical difficulty or there could be something wrong with our processes. Other standards bodies meet their deadlines but they put out documents with certain items still open for study. These documents aren't usable by implementers. We don't do that. It can be frustrating for other organizations, but it has always been the IETF practice to wait until we have a standard that can be implemented.

What concerns you most about the health of the Internet infrastructure?

Where [Multi-protocol Label Switching] and [Generalized MPLS] go are clearly a matter of concern. We still have security issues at the infrastructure level, including securing [Border Gateway Protocol]. Internationalization is also a very interesting issue because it's a matter of great interest to the users. But it's a matter of very little interest to some of the technical people because they view it as a presentation-layer issue.

There is a perception that more of the cutting-edge standards work is going to other groups, such as the Organization for the Advancement of Structured Information Standards and the Liberty Project. Is the IETF losing the cool work to rival standards bodies?

It's clear that one of the things we need to do is understand the scope of what we do in the applications area. For example, in the area of Web services, a lot of standards work is done by the World Wide Web Consortium and OASIS. I don't think that's a point of tension. Everyone agrees that the IETF is the maintenance body for [Hypertext Transfer Protocol], while everything that runs on HTTP is at W3C. There's some virtue in specialization for the standards bodies. So I don't believe we're losing the cool work.

Is the IETF still the Internet's premier standards-setting body?

Yes. I believe it is for infrastructure standards. For Layers 3 and 4, we are the leaders. I don't believe that's in doubt.

Attendance at this meeting is down, from a high of 3,000 a few years ago to a little more than 1,000 now. How big of a problem is that?

What I'm hearing is that things are working much better than when we had 3,000 attendees and people were spilling out into the hallways. Now the people who come to our meetings are serious about the work we do.

Your predecessor, Harald Alvestrand of Cisco, spent much of the past two years involved in administrative restructuring. Do you think you will, too?

What I'm hoping is that we can fairly expeditiously finish administrative restructuring and get the new administrative oversight committee in place so it can become a self-contained entity. I will still be concerned about IETF workflow, IETF processes and IETF sociology. Part of my job is to make sure all of that runs smoothly.

The IETF chair is a huge job with no pay and lots of hassles. Why take on this job?

Partly because people were twisting my arm, but mostly because I think it's important to grow the Internet for the benefit of the whole world.

AT&T, MCI and Sprint have traditionally been active participants in the IETF but they are all undergoing mergers. The regional carriers — SBC, Verizon and Qwest — have not been as active in the IETF. Will ISP consolidation hurt the IETF?

That's a hard question. Larger companies tend to move more slowly to new technology, but when they move they really throw their weight around. The question is when these carriers will need to upgrade. The smaller carriers have tended to be end users rather than innovators in the technology. Once the acquisitions shake down, I can't see how they won't be interested in new technologies. ■

■ See how the IETF is approaching communication over the Internet in the event of emergencies. PAGE 63.

NetworkWorld

EDITORIAL DIRECTOR: JOHN GALLANT
EDITOR IN CHIEF: JOHN DIX

■ NEWS
EXECUTIVE EDITOR, NEWS: BOB BROWN
ASSOCIATE NEWS EDITOR: MICHAEL COONEY
ASSOCIATE NEWS EDITOR: PAUL MCNAMARA

■ NET INFRASTRUCTURE
SENIOR EDITOR: JOHN COX (978) 834-0554; Fax: (978) 834-0558
SENIOR EDITOR: TIM GREENE
SENIOR EDITOR: PHIL HOCHMUTH
SENIOR EDITOR: ELLEN MESSMER, (941) 792-1061

■ ENTERPRISE COMPUTING
SENIOR EDITOR: JOHN FONTANA (303) 377-9057; Fax: (303) 377-9059
SENIOR EDITOR: DENI CONNOR (512) 345-3850; Fax: (512) 345-3860
SENIOR EDITOR: JENNIFER MEARS, (608) 836-8490; Fax: (608) 836-8491

■ APPLICATION SERVICES
SENIOR EDITOR: CAROLYN DUFFY MARSAN, (703) 917-8621; Fax: (703) 917-8622
SENIOR EDITOR: ANN BEDNARZ (612) 926-0470
SENIOR EDITOR: DENISE DUBIE
SENIOR EDITOR: CARA GARRETSON, (240) 246-0098

■ SERVICE PROVIDERS
SENIOR EDITOR: DENISE PAPPALARDO, (703) 768-7573
MANAGING EDITOR: JIM DUFFY (716) 655-0103

■ NET.WORKER
MANAGING EDITOR: TONI KISTNER, (617) 868-6624

■ COPY DESK/LAYOUT
MANAGING EDITOR: RYAN FRANCIS
COPY CHIEF: BRETT COUGH
SENIOR COPY EDITOR: JOHN DOOLEY
COPY EDITOR: MONICA HAMILTON
ASSOCIATE COPY EDITOR: KYLE CONNORS

■ ART
DESIGN DIRECTOR: TOM NORTON
ART DIRECTOR: BRIAN GAIDRY
SENIOR DESIGNER: STEPHEN SAUER
ASSOCIATE DESIGNER: ERIC ANDERSON

■ FEATURES
FEATURES EDITOR: NEAL WEINBERG
SENIOR MANAGING EDITOR, FEATURES: AMY SCHURR
OPINIONS PAGE EDITOR: SUSAN COLLINS

■ CLEAR CHOICE TESTS
EXECUTIVE EDITOR, TESTING: CHRISTINE BURNS, (609) 683-4432
SENIOR EDITOR, PRODUCT TESTING: KEITH SHAW, (508) 490-6527
LAB ALLIANCE PARTNERS: JOEL SNYDER, Opus One; JOHN BASS, Centennial Networking Labs; BARRY NANCE, independent consultant; THOMAS POWELL, PINT; Miercom; THOMAS HENDERSON, ExtremeLabs; TRAVIS BERKLEY, University of Kansas; DAVID NEWMAN, Network Test; CHRISTINE PEREY, Perey Research & Consulting; JEFFREY FRITZ, University of California, San Francisco; JAMES GASKIN, Gaskin Computing Services, MANDY ANDRESS, ArcSec; RODNEY THAYER, Canola & Jones
CONTRIBUTING EDITORS: DANIEL BRIERE, MARK GIBBS, JAMES KOBIELUS, MARK MILLER

■ NETWORK WORLD FUSION
EXECUTIVE EDITOR, ONLINE: ADAM GAFFIN
MANAGING EDITOR: MELISSA SHAW
MANAGING EDITOR, ONLINE NEWS: JEFF CARUSO, (631) 584-5829
ASSOCIATE ONLINE NEWS EDITOR: LINDA LEUNG, (510) 768-2808
MULTIMEDIA EDITOR: JASON MESERVE
SENIOR ONLINE COPY CHIEF: SHERYL HODGE
SENIOR ONLINE GRAPHIC DESIGNER: ZACH SULLIVAN

■ SIGNATURE SERIES
EDITOR: BETH SCHULTZ, (773) 283-0213; Fax: (773) 283-0214
EXECUTIVE EDITOR: JULIE BORT, (970) 482-6454
COPY EDITOR: BRETT COUGH

EDITORIAL OPERATIONS MANAGER: CHERYL CRIVELLO
OFFICE MANAGER, EDITORIAL: GLENNA FASOLD
EDITORIAL OFFICE ADMINISTRATOR: PAT JOSEFEK
MAIN PHONE: (508) 460-3333
E-MAIL: first name_last name@nww.com

THE BRAINS TO BACK IT UP.

A lot of products claim to reduce the complexity and cost of enterprise backup. But one actually delivers—the Scalar® i2000, part of the growing iPlatform™ family from ADIC, the leading provider of tape libraries for open-systems backup.*

Embedded intelligence. The Scalar i2000 is the first library to integrate advanced management functions—proactive monitoring, built-in partitioning, automated diagnostics, and I/O management—so it delivers faster and more reliable backup and uses less of your budget, time, and staff.

Faster resolution, fewer service calls. Smarter diagnostics and dedicated service teams mean fewer interruptions and faster resolution. The Scalar i2000 requires half the service calls of conventional libraries. And the worldwide ADIC service team solves problems before customers see them.

Capacity on demand. As its name suggests, the Scalar i2000 is designed to scale with your storage needs. So you don't have to worry about running out of space or paying for more than you need.

After all, you were hired to use your brains for more important things.

*Market share from Gartner Dataquest, Tape Automation Systems Market Shares, 2003, F. Yale, April 2004.

Visit www.adic.com/i2k to get your free Aberdeen Group white paper:
Taking an Intelligent Step Forward in Tape Backup and Restore.

adic
Intelligent Storage™

Available through EMC Corporation, your complete source for information lifecycle management solutions. Call your local ADIC or EMC sales representative for more information.

Copyright 2005 Advanced Digital Information Corporation (ADIC), Redmond, WA, USA. All rights reserved. Created in USA.

EMC²
where information lives™

Stage set for compromise on IEEE high-speed

■ BY JOHN COX

ATLANTA — The IEEE task group charged with creating a 100M bit/sec wireless LAN standard has set the stage for a compromise between the two remaining factions.

Members of the TGn Sync and World Wide Spectrum Efficiency (WWiSE) organizations might be ready to negotiate on a proposal that could win 75% of the votes at the next meeting of 802.11n task group. That's the number needed for a proposal to be adopted as a draft standard. Otherwise, the group will take a step backward and begin to reconsider proposals that had been eliminated.

The group's job is to create a WLAN standard that will deliver actual throughput of more than 100M bit/sec, a quantum leap above the 20M bit/sec for today's 802.11g and 11a WLANs. The current 802.11 standard eats up more than half of the 54M bit/sec data rate for 802.11g and 11a. The higher, though still shared, bandwidth will rival that of many wired networks and support demanding applications such as several video and audio streams at once, huge image files and simulations.

"Both sides realize that a standard has to come as quickly as possible," says Jack Winters, chief scientist at Motia, a Pasadena, Calif., fabless semiconductor company designing radio chips that integrate with smart antennas. Winter is a member of the 802.11n task group but is not affiliated with TGn Sync or WWiSE. "Delays or deadlocks will result in both groups failing," he says.

Last week in Atlanta, members of the 802.11n task group continued winnowing proposals. They voted by a slender majority in favor of one proposal from a group of vendors called TGn Sync. But the next day, in the confirmation vote, that proposal fell far short of the 75% majority it needed to be adopted as the draft 802.11n standard.

The members of TGn Sync include chip makers such as Atheros, Intel and Marvel, network equipment makers such as Cisco and Nortel, and consumer products companies such as Panasonic, Samsung and Sony. WWiSE members include Airgo Networks, Broadcom, Connexant, Motorola and Texas Instruments, along with Buffalo Technology, Hughes Network Systems, France Telecom, Nokia and NTT.

Both proposals (details at www.nwfusion.com, DocFinder: 6353) make use of technology called multiple input/multiple output (MIMO) to dramatically boost the amount of data that can be sent over a radio connection. MIMO-based WLAN products already are on the market based on Airgo's chipset, which is the only one shipping in volume. (See related story on page 67.)

"Neither one has the votes for 75% right now, unless there's an official compromise," says Greg Raleigh, CEO of Airgo, and author of one of the earliest academic papers on MIMO. "We're not even at Draft 1.0 yet. And after that, you have to design [a standard] that you can actually build [products] to, and interoperate."

There already has been compromise, Motia's Winters says, as both groups have made changes in their proposals. TGn Sync dropped a requirement to use 40-MHz channels instead of the conventional 20 MHz; now the bigger channel is an option. WWiSE added support for transmit beam forming, which is a technique for boosting performance by using antenna arrays that in effect focus radio signals. ■

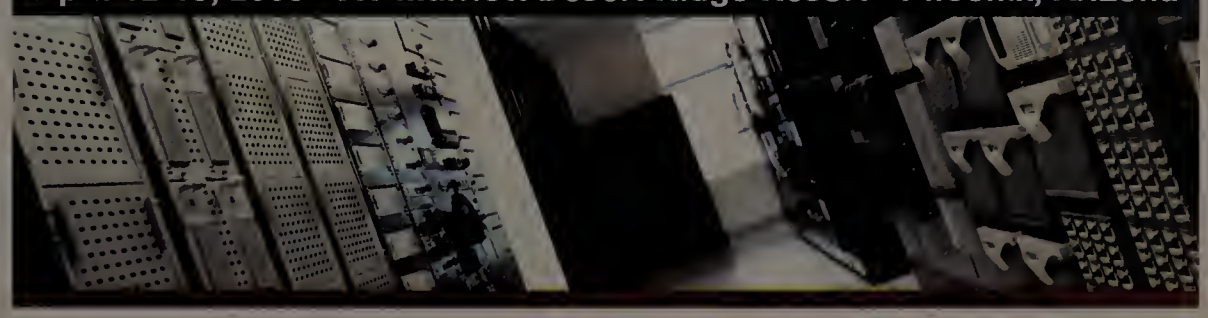
SNIA

STORAGE NETWORKING WORLD

COMPUTERWORLD

Learn How to Achieve Storage Networking Success

April 12-15, 2005 • JW Marriott Desert Ridge Resort • Phoenix, Arizona



Featured Speakers Include:

BOB LOGAN
Vice President, Enterprise Infrastructure Services
SAIC

SONJA ERICKSON
Vice President, Technical Operations
Kodak EasyShare Gallery

SASAN HAMIDI
CSO
Interval International

STEVE DUPLESSIE
Founder and Senior Analyst
Enterprise Strategy Group

JON WILLIAM TOIGO
CEO and Founder
Toigo Partners International

ANN LIVERMORE
Executive Vice President, Technology Solutions Group
Hewlett-Packard Company

See and Hear Ira Winkler

IRA WINKLER
Expert in Corporate and Computer Security
Author of *Spies Among Us: How to Stop the Spies, Terrorists, Hackers and Criminals You Don't Even Know You Encounter Every Day*

The Leading Conference for:

- IT Management
- Storage Architects
- IT Infrastructure Professionals
- Business Continuity Planning Experts
- Data Management Specialists
- Network Professionals

To register or for more information, visit **www.snwusa.com/nww**

See solutions from companies including: (as of 3/8/05)

PLATINUM SPONSORS

adic Intelligent Storage™ · BROCADE · Cisco Systems · CommVault · Computer Associates · DLT · dotHILL · EMC² where information lives · EMULEX · hp invent · HITACHI DATA SYSTEMS · IBM · intel · LSI LOGIC · McDATA · Microsoft · QLOGIC · Quantum · Seagate · StorageTek · Sun · symantec. · Xiotech

GOLD SPONSORS

adaptec · AppIQ · BLUE ARC · DELL · engenio · FCIA · Gateway · ISILON · NetApp · Overland STORAGE · sgi · SPECTRA LOGIC · syncsort · verizon · VITESSE · WilTel · XOsoft · xyratex

CONTRIBUTING SPONSORS

3PAR · acopia · Agilent Technologies · ARSENAL · AVAMAR · CENTREPATH · CNT · Data Domain · DECRU · DILIGENT · FalconStor · Hifn · Infortrend · LeftHand NETWORKS · maranti · neartek · NTP Software · ONARO · PMC · Rainfinity · revivio · RIVERBED · SBE · Servergraph · TACIT · Topio

MEDIA SPONSORS

Bio-IT World · Business Solutions · COMPUTERWORLD · Data Storage Connection · IDC · Storage Security · INFOSTOR · InfoWorld · Integrated Solutions · Jobstor.com · Network World · Sys Admin

"BEST PRACTICES" AWARDS PROGRAM SPONSORED BY: EMC² where information lives

PARTNER PAVILION: Microsoft · DLT

GOLF OUTING SPONSOR: Quantum

For sponsorship opportunities, call Ann Harris at 508-820-8667

The first 800 qualified IT End-Users who register and attend SNW will receive a free copy of

Spies Among Us by Industry Visionary, Ira Winkler

Co-Owned and Endorsed by SNIA

Co-Owned and Produced by COMPUTERWORLD

"... networking ..."

Michael Dugan
Director of Technology,
Forbes.com

"... the premier event in the storage industry ..."

Frank Enfanto
Vice President,
Operations Delivery &
Information Security,
Blue Cross Blue Shield
of Massachusetts

SNIA

STORAGE NETWORKING WORLD

COMPUTERWORLD

Co-Owned and Endorsed by SNIA

Co-Owned and Produced by COMPUTERWORLD

Learn How to Achieve Storage Networking Success

- Get a contemporary overview of today's storage networking issues and opportunities
- See how to implement and deploy the latest in storage networking technologies
- Hear the latest in enterprise security
- Learn from best practices and case studies

Why You Should Attend

Are you responsible for managing your company's data center assets? Want to exchange innovative ideas and strategies with other executives who share the same objectives? Then attend Storage Networking World, where you'll network with and learn from renowned experts and the nation's top user executives.

Conference At-a-Glance *(subject to change)*

For details, updates, and to register visit **www.snwusa.com/nww**

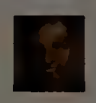
TUESDAY, APRIL 12

Registration Open 11:00am - 8:30pm

9:00am – 9:30am	Breakfast
9:30am – 11:30am	**Pre-Conference Tutorials and Primers**
11:30am – 1:00pm	Luncheon
12:00pm – 5:00pm	**Pre-Conference Golf Outing**
1:00pm – 5:25pm	**End-User Case Studies; SNIA Voice of the User Track; SNIA Technical Tutorials Track; Deployable Solutions Track**
6:00pm – 8:00pm	Welcome Reception

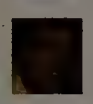
WEDNESDAY, APRIL 13

Registration Open 7:00am - 8:00pm

7:15am – 8:15am	Breakfast
8:15am – 8:30am	**Opening Remarks**
8:30am – 9:15am	 **Opening Visionary Presentation** Ira Winkler, Security Expert and Author of *Spies Among Us*
9:15am – 9:45am	 **End-User Case Study** Bob Mathers, Second Vice President, Information Technology Operations & Disaster Recovery, Guardian Life Insurance
9:45am – 10:15am	 **Industry Leader Presentation** Ann Livermore, Executive Vice President, Technology Solutions Group, Hewlett-Packard Company
10:15am – 10:30am	Break
10:30am – 11:00am	 **End-User Case Study** Bob Eicholz, Vice President, EFILM, LLC
11:00am – 11:30am	 **Industry Leader Presentation** John Thompson, CEO, Symantec
11:30am – Noon	 **End-User Case Study: The Story (and Storage!) Behind Kodak's Online Photo Success** Sonja Erickson, Vice President, Technical Operations, Kodak EasyShare Gallery
Noon – 12:45pm	 **Panel Discussion** Moderated by: Jon William Toigo, CEO & Founder, Toigo Partners International
12:45pm – 2:00pm	Luncheon
2:10pm – 5:40pm	**End-User Case Studies; SNIA Voice of the User Track; SNIA Technical Tutorials Track; Deployable Solutions Track**
5:40pm – 8:40pm	**Expo with Dinner and Interoperability & Solutions Demo** • 30-plus SNIA member companies collaborating on integrated solutions • Opportunity to meet leading experts and engineers

THURSDAY, APRIL 14

Registration Open 7:00am - 6:00pm

7:15am – 8:15am	Breakfast
8:15am – 8:30am	**Opening Remarks**
8:30am – 9:15am	**Opening End-User Visionary Presentation**
9:15am – 9:45am	 **Industry Leader Presentation** Andy Monshaw, General Manager, Storage Systems, IBM Systems and Technology Group
9:45am – 10:15am	 **End-User Case Study** Bob Logan, Vice President, Enterprise Infrastructure Services, SAIC
10:15am – 10:30am	Break
10:30am – 11:00am	 **Industry Leader Presentation** Jeff Nick, Vice President and Corporate-Wide CTO, EMC Corporation
11:00am – 11:30am	 **End-User Case Study** Sasan Hamidi, CSO, Interval International
11:30am – Noon	 **Industry Leader Presentation** John Kelley, President and CEO, McData
Noon – 12:45pm	 **End-User Panel** Moderated by: Steve Duplessie, Founder & Senior Analyst, Enterprise Strategy Group
12:45pm – 2:00pm	Expo with Lunch and Interoperability Demo
2:10pm – 5:40pm	IDC **Storage Analyst Briefing**
2:10pm – 5:40pm	**End-User Case Studies; SNIA Voice of the User Track; SNIA Technical Tutorials Track; Deployable Solutions Track**
4:00pm – 7:00pm	**Expo Open** • Cocktail Reception in Expo begins at 5:30pm
7:00pm – 9:30pm	**Gala Evening with Awards Ceremony, Dinner & Entertainment**

FRIDAY, APRIL 15

Registration Open 7:30am - 10:00am

7:30am – 10:00am	Continental Breakfast
8:30am – Noon	**End-User Case Studies; SNIA Voice of the User Track; SNIA Technical Tutorials Track; Deployable Solutions Track**
Noon	Conference Concludes

"... at SNW, you connect with folks you normally wouldn't meet and capitalize on the serendipitous exchange of ideas ..."

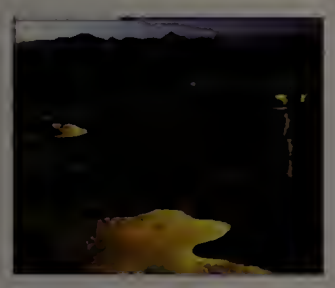
John Seely Brown
former director, Xerox Palo Alto Research Center (PARC), and former chief scientist, Xerox

"... SNW is a great venue for peer discussion ... an opportunity to provide feedback to vendors on what users need from them ..."

John Greer
Director, IT Infrastructure, Pacific Gas & Electric

SNIA

Attend SNIA-Certified Training Programs at SNW
Visit www.snwusa.com for more information.



The Wildfire Golf Club, Faldo Course
Phoenix, Arizona

JW Marriott Desert Ridge Resort
Phoenix, Arizona

Pre-Conference Golf Outing
Complimentary for Registered IT End-Users

SPONSORED BY **Quantum**

The Pre-Conference Golf Outing at The Wildfire Golf Club, Faldo Course located at the JW Marriott Desert Ridge Resort, is complimentary ($165 value) for registered IT End-Users (other participants, including sponsors and vendors, may play on an "as available" basis and are responsible for all applicable golf outing expenses).

For details contact Chris Leger at 1-508-820-8277

Hotel Reservations and Travel Services

Global Odysseys is the official travel company for Storage Networking World. They are your one-stop shop for exclusive discounted rates on hotel accommodations.

To reserve your accommodations, visit: **www.etcentral.com**

You can also call our conference housing line at: **1-888-254-1597**

SNIA

STORAGE NETWORKING WORLD

COMPUTERWORLD

April 12-15, 2005
JW Marriott
Desert Ridge Resort
Phoenix, Arizona

Application for Conference Registration

Fax this completed application to 1-508-820-8254 or apply online at: www.snwusa.com/nww

Your business card is REQUIRED to process your application

Please affix your business card to this space prior to submitting your application. Applications submitted without business cards will not be processed.

Questions? Call 1-800-883-9090

If not indicated on your business card, please provide the following required information:

Corporate Email Address

Corporate Website

Registration questions?
Call 1-800-883-9090 or email
snwreg@computerworld.com

Need accommodations?
Reserve them at: **www.etcentral.com**
Or call 1-888-254-1597
or email: eventhousing@globalodysseys.com

Please check ONE of the following:	**Earlybird Registration** (through February 28, 2005)	**Full/Onsite Registration** (after February 28, 2005)
❑ **I am an IT End-User*** **(Complete Attendee Profile below)**	❑ **$895** General Conference Package (April 13 & 14) (includes General Conference Sessions, Expo, Meals & Receptions) ❑ **$1,290** Total 4-Day Package (April 12, 13, 14, 15) (includes General Conference, plus Technical and Business Tracks, SNIA-produced Tutorials, SNIA-Certification "Test-Ready" Courses)	❑ **$1,295** General Conference Package (April 13 & 14) (includes General Conference Sessions, Expo, Meals & Receptions) ❑ **$1,690** Total 4-Day Package (April 12, 13, 14, 15) (includes General Conference, plus Technical and Business Tracks, SNIA-produced Tutorials, SNIA-Certification "Test-Ready" Courses)

* IT End-Users are defined as those who are attending Storage Networking World with an intent (and an IT spending budget) to potentially buy/lease hardware/software/services, etc. from our conference sponsors and are not themselves an IT vendor. As such, account representatives, business development personnel, analysts, consultants and anyone else attending who does not have IT purchasing influence within their organization are excluded from the "IT End-User" designation. Interpretation and enforcement of this policy are at the sole discretion of Computerworld.

❑ **I am a Channel Partner/ Integrator/Consultant** **(Complete Attendee Profile below)**	❑ **$3,000** Total 4-Day Package (April 12, 13, 14, 15) (includes General Conference; Technical and Business Tracks, SNIA-produced Tutorials, SNIA Certification "Test-Ready" Courses)	❑ **$3,500** Total 4-Day Package (April 12, 13, 14, 15) (includes General Conference; Technical and Business Tracks, SNIA-produced Tutorials, SNIA Certification "Test-Ready" Courses)

By participating in SNW's Channel Partner/Integrator registration package, registrants may enjoy the following benefits: One company representative may receive a full conference pass to SNW Spring 2005; additional company representatives pay $695 each for full conference passes; company may invite up to five IT User customers to attend SNW Spring(IT Users must be strictly compliant with IT User definition on the supplied registration form); companies registering for this package interested in joining the SNIA are eligible to receive a $2,000 discount, provided that membership is applied for prior to March 1, 2005.

Attendee Profile: This section MUST be completed by IT End-Users and Channel Partners/Integrators/Consultants only (optional for all other registrations) in order to process your application.

Your Business/Industry
- ❑ Aerospace
- ❑ Manufacturing & Process Industries (non-computer related)
- ❑ Finance/Banking/Accounting
- ❑ Insurance/Real Estate/Legal Sevices
- ❑ Government: Federal (including Military)
- ❑ Government: State or Local
- ❑ Health/Medical/Dental Services
- ❑ Retailer/Wholesaler/Distributor (non-computer related)
- ❑ Transportation/Utilities
- ❑ Communication Carriers (ISP, Telecom, Data Comm, TV/Cable)
- ❑ Construction/Architecture/Engineering
- ❑ Data Processing Services
- ❑ Education
- ❑ Agriculture/Forestry/Fisheries
- ❑ Mining/Oil/Gas
- ❑ Travel/Hospitality/Recreation/Entertainment
- ❑ Publishing/Broadcast/Advertising/ Public Relations/Marketing
- ❑ Research/Development Lab
- ❑ Business Services/Consultant (non-computer related)
- ❑ Manufacturing of Computers, Communications, Peripheral Equipment or Software

Your Job Title/Function:
IT MANAGEMENT
- ❑ CIO, CTO, CSO
- ❑ Executive VP, Senior VP
- ❑ Vice President
- ❑ Director
- ❑ Manager/Other IT Manager
- ❑ Supervisor

BUSINESS MANAGEMENT
- ❑ CEO, COO, Chairman, President
- ❑ CFO, Controller, Treasurer
- ❑ Executive VP, Senior VP, VP, General Manager
- ❑ Director, Manager
- ❑ Other Corporate/Business Manager

Number of employees in your entire organization (ALL locations)
- ❑ 20,000 or more
- ❑ 10,000 - 19,999
- ❑ 5,000 - 9,999
- ❑ 1,000 - 4,999
- ❑ 500 - 999
- ❑ 100 - 499
- ❑ 50 - 99
- ❑ Less than 50

What is your organization's annual IT/IS budget for all IT/IS products?
- ❑ $1 Billion or more
- ❑ $500 Million - $999.9 Million
- ❑ $100 Million - $499.9 Million
- ❑ $50 Million - $99.9 Million
- ❑ $10 Million - $49.9 Million
- ❑ $1 Million - $9.9 Million
- ❑ $500,000 - $999,999
- ❑ $250,000 - $499,999
- ❑ $100,000 - $249,999
- ❑ Less than $100,000

What is the estimated annual revenue of your entire organization?
- ❑ Over $10 Billion
- ❑ $1 Billion - $9.9 Billion
- ❑ $500 Million - $999 Million
- ❑ $100 Million - $499 Million
- ❑ Less than $100 Million

The one item that best describes your involvement in the IT purchase process
- ❑ Authorize/approve purchase
- ❑ Evaluate/recommend products, brands, vendors
- ❑ Specify features/technical requirements
- ❑ Set budget for expenditures
- ❑ Determine need to purchase
- ❑ Create IT strategy
- ❑ All of the above

Would you like to receive information about playing in the golf outing on Tuesday, April 12th?
- ❑ Yes
- ❑ No

Do you need hotel accomodations?
- ❑ Yes (please visit www.etcentral.com to reserve)
- ❑ No

Would you like to receive a complimentary subscription to Computerworld?
- ❑ Yes
- ❑ No

❑ **My company is Sponsoring/ Exhibiting at SNW**	❑ **$895** (through February 28, 2005) General Conference Package (April 13 & 14) (includes General Conference Sessions, Expo, Meals & Receptions) ❑ **$1,290** Total 4-Day Package (April 12, 13, 14, 15) (includes General Conference, plus Technical and Business Tracks, SNIA-produced Tutorials, SNIA-Certification "Test-Ready" Courses)	❑ **$1,295** (after February 28, 2005) General Conference Package (April 13 & 14) (includes General Conference Sessions, Expo, Meals & Receptions) ❑ **$1,690** Total 4-Day Package (April 12, 13, 14, 15) (includes General Conference, plus Technical and Business Tracks, SNIA-produced Tutorials, SNIA-Certification "Test-Ready" Courses)

As a sponsor, you may be eligible to attend using a registration provided with your sponsorship. (If those registrations have already been assigned/used, then you may register at the prevailing rates above.) See the current list of sponsors at www.snwusa.com. Questions? Call 1-800-883-9090 or email snwreg@computerworld.com.

❑ **I am a representative of a Non-Sponsoring IT Vendor Company**
❑ **$5,000 Business Development Professional Package** for Sales, Marketing and Business Development Professionals (includes General Conference Sessions, Expo, Meals & Receptions)

Vendors are encouraged to participate in Storage Networking World through sponsorship. (Details are available by calling Ann Harris at 508-820-8667.) Alternatively, vendors (as well as other "non-IT end-user" professionals as defined by Computerworld), may apply for registration at the "non-sponsoring vendor" rate of $5,000. Determination of what constitutes a "non-sponsoring vendor" registration is made exclusively by Computerworld.
Please call 888-239-4505 with questions.

❑ **I am a Financial/Equity Analyst and/or Venture Capital Professional**

❑ **$1,290** (through February 28, 2005) General Conference Package (includes General Conference Sessions, Expo, Meals & Receptions)	❑ **$1,690** (after February 28, 2005) General Conference Package (includes General Conference Sessions, Expo, Meals & Receptions)

❑ **I am a qualified member of the press.** I can verify my press credentials.
Press should call Marenghi Public Relations at 1-781-915-5000 to register.

Please fax this completed application to 1-508-820-8254

Payment Method

❑ **Check** (checks must be received by March 21, 2005 payable to: Computerworld) Mail to: Computerworld, Attn: Mike Barbato, One Speen Street, Framingham, MA 01701

❑ **American Express** ❑ **VISA** ❑ **MasterCard**

Account Number:_____

Expiration Date:_____

Card Holder Name:_____

Signature of Card Holder:_____

Cancellation Policy (All of the following require **written notification** by March 21, 2005)
In the event of cancellation, the registrant has three options:
1) He or she may substitute another attendee for this conference.
2) He or she may transfer this registration to the Storage Networking World Fall 2005 conference.
3) The registration fee will be refunded, less a $250 service charge (if written notice is received by March 21, 2005).
Please send cancellation requests via email to: snwreg@computerworld.com

Net Infrastructure

■ SECURITY ■ SWITCHING ■ ROUTING
■ VPNS ■ BANDWIDTH MANAGEMENT
■ VOIP ■ WIRELESS LANS

Short Takes

■ **NetPro, Oblix, Oxford Computer Group, PointBridge** and **Vintela** last week formed the MIIS Alliance to help corporations manage identities using **Microsoft Identity Integration Server.** Alliance members will offer services and products that complement to one another and the Microsoft platform focusing on infrastructure management, implementation services, corporate identity and Web services management, and platform integration. MIIS is a cornerstone in Microsoft's identity management platform, which also includes Active Directory.

■ **NFR Security** last week announced it will add what it calls "dynamic shielding" to its Sentivist intrusion-prevention system. The feature lets the company's IPS sensor provide more detailed information about application vulnerabilities by accepting input from the Nessus and Nevo open source vulnerability scanners. The dynamic shielding capability will be a software upgrade to the Sentivist IPS and won't affect its price, which is $13,000 per sensor.

■ **McAfee** last week introduced a tool to help customers manage the company's corporate security software. **ProtectionPilot** is aimed at reducing administration time by centrally deploying and managing security updates. It also lets administrators check for malware infections and locate out-of-date systems through its Interactive Security Dashboard. The tool supports McAfee's SMB Edition security software suites, which include anti-virus protection for desktops and file servers. McAfee's standalone Anti-Spyware enterprise product also can be managed using ProtectionPilot, the company says. ProtectionPilot with McAfee Active Virus Defense SMB Edition, which includes virus scanning for gateways, servers, workgroups and desktops, is about $919 for a five-node pack. Pricing for McAfee Active VirusScan SMB Edition with ProtectionPilot wasn't announced.

CipherTrust bolsters compliance

■ BY CARA GARRETSON

E-mail security vendor CipherTrust announced last week an upgrade to its gateway appliance with a compliance control feature designed to help customers adhere to regulatory and corporate policies.

IronMail 5.0, available later this month, will feature CipherTrust's Compliance Control that scans an organization's outgoing mail for content that should not leave the company per corporate policy or government regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley, company officials say.

The compliance feature will come standard with Version 5.0, which is priced starting at $20,000. Companies also can opt for a dedicated version of IronMail that performs only compliance monitoring and costs $25,000.

CipherTrust joins a number of e-mail security vendors such as MailFrontier, FrontBridge Technologies, Barracuda Networks, Proofpoint and IronPort Systems in including compliance features to their messaging offerings. As companies filter incoming mail for viruses, spam and other messaging abuses, it makes sense to use the same products to scan outbound messages to ensure sensitive information isn't leaving the corporate network, one analyst says.

"I do believe there are advantages to an all-in-one approach; it allows services to run off a common infrastructure and produces operational efficiencies so there's one common console to manage all of these different disciplines," says Matt Cain, an analyst with Meta Group.

With Compliance Control, CipherTrust has upgraded the content filtering dictionaries included with its appliance to include terms and phrases associated with specific regulations and to spot patterns associated with sensitive material. For example, Compliance Control scans outgoing mail for text containing terms that are associated with documents covered by HIPAA, such as "medical provider." It also can detect patterns such as the number and spacing of digits used in Social Security numbers and credit card numbers, officials say.

The policies also can be customized to detect company-defined patterns, according to officials.

These capabilities work with IronMail's current outbound mail techniques, such as scanning of attachments and encrypted messages, designed to help protect companies from violating regulations or losing sensitive information.

From an administrative standpoint, Compliance Control is designed to be managed by a company's compliance officer, therefore taking the burden off the IT administrator, officials say. Messages flagged by Compliance Control can be held in quarantine until the compliance officer clears them. ■

Start-up to manage Exchange systems

■ BY JOHN FONTANA

Start-up Azaleos this week will debut itself and its appliance aimed at helping users create a highly-available and remotely-managed Microsoft Exchange platform.

Azaleos' OneServer is a dedicated appliance that provides an active/passive, fault tolerant and clustered Exchange platform for corporate messaging. The appliance, which is built on either HP or Dell hardware, runs Windows Server 2003 and Exchange 2003 and is complemented by security, mobility and compliance software from third-party vendors.

The server, which is focused on fortifying the Exchange message store, is deployed within a corporation's network yet managed remotely by Azaleos. User management tasks, such as password changes and message store limits, are still done by corporate administrators through OneServer's Web-based administrative console.

Azaleos' OneStop Subscription Service is coupled in the OneServer package. It includes 24-7 monitoring along with maintenance and management of the appliance from the hardware to patch management on Windows, Exchange and third-party software within OneServer. Azaleos tests the patches using a replica of the customer's OneServer environment before pushing them out to OneServer, which has a rollback feature to eliminate downtime.

> **"Exchange can be a challenging platform to keep up and running."**
>
> **Mark Levitt**
> Analyst, IDC

"Exchange can be a challenging platform to keep up and running," says Mark Levitt, an analyst at IDC. He says IDC research has shown a "hefty management load" for the older Exchange platforms, versions 5.5 and 2000. "Any way a company can get help to deal with patches and upgrades, and identify potential problems as they are developing will save them time and money. Doing that with an appliance is not typical for top-tier software, but it reflects the fact that keeping corporate e-mail systems running smoothly with minimal down time is not an easy thing," Levitt says.

While the OneServer is a unique approach to solving that issue, Azaleos faces competition from third-party Exchange management software vendors such as Quest, NetIQ and other start-ups, including Lucid8 Information Systems.

But Azaleos' angle is one that should be familiar to large organizations, according to its founders.

"Think about this in the context of how today people deploy storage devices, boxes that sit in network and push out monitoring information," says Keith McCall, co-founder and CTO of Azaleos. "We are doing the same thing for enterprise

See Azaleos, page 19

Symantec evaluates threat potential

Bombardment of phish scams, viruses and worms increases, according to Symantec's latest report.

■ BY ELLEN MESSMER

Phishing scams and Windows32-based viruses and worm variants are on the rise, according to Symantec, which this week will publish its semiannual Internet Security Threat Report.

The report — which looks at trends between last July and December — garners its research data from Symantec's network of 20,000 sensors, its BrightMail anti-spam service and 2 million "decoy" mailboxes around the world. There were 10,310 phishing scams sighted during the six months the security report covers. Symantec says the number of phishing messages sent to intended victims rose from 9 million per week in July to 33 million in December.

"These fake Web sites and e-mail scams are seeking personal identifiable information," says Jonah Paransky, senior manager of security product management at Symantec. By using phishing tactics, criminals intend to steal personal information and use it for monetary gain, he points out.

The number of Win32 viruses and worm variants also continues to climb, with the six-month period under review showing 65% more viruses reported than the one before, for a total of 7,360 new viruses and worms.

As of Dec. 31, 2004, the total number of Win32 viruses and worms approached 17,500, which Symantec says could compel organizations to update anti-virus resources.

There weren't many numbers in the Internet Security Threat Report that might make IT managers happy. The number of average attacks per day on individual organizations went up from an average of 10.6 to an average of 13.6 attacks per day. One of the few numbers that went down reflects the time between the disclosure of a vulnerability and the release of an associated exploit — 5.8 days to 6.4 days. "We got an extra day to prepare, such as [by] patching," Paransky says.

Both Microsoft and open source applications showed some holes. Symantec noted that 21 vulnerabilities were spotted in the Mozilla browser compared with 13 vulnerabilities affecting Microsoft Internet Explorer.

For the first time in its Internet Security Threat Report, Symantec began looking at adware, the type of spyware programs used in marketing, which can cause computer slowdowns and privacy compromise.

A program called Webhancer, which monitors visited Web sites, and Iefeats, which modifies a start page, were two of the most-sighted adware programs, according to Symantec.

Spyware, which also can refer to malicious Trojans and keyloggers, is a broad term subject to various interpretations. Symantec's rival, McAfee, prefers not to use the term spyware, but instead to refer to adware and the like as "potentially unwanted programs."

Symantec, which intends to introduce enterprise anti-spyware products later this year, says it has come up with a way to distinguish and classify the array of troublesome code raining down on Internet users from Web site downloads or e-mail.

"We want to start changing the conversation to be centered around risk," says Vincent Weafer, senior director of Symantec's Security response group, about spyware. "These programs produce a security risk. And in the research labs, we're looking at the functionality of these programs and putting them in categories."

Symantec's risk-impact model is based on five metrics to be applied to spyware: the performance impact on computer system performance; the privacy impact; how hard it is to remove it; the relative stealth of the code in installation and concealment; and the prevalence of it.

Weafer says a rating of high, medium and low can be applied to each of these categories. This categorization of spyware code, and the concept of authorization vs. non-authorization, is expected to factor into the design of Symantec's anti-spyware software. ■

Threat report

Between July 1 and Dec. 31, 2004, Symantec found:

- 10,310 new phishing scams.
- 9 million phishing messages per week in July, rising to 33 million per week in December.
- 60% of all e-mail traffic was spam.
- Attack trends showed organizations facing 13.6 attacks per day vs. 10.6 the previous six months.
- 7,360 new Win32 viruses and worm variants, up 64% from before.

Figures are derived from Symantec's DeepSight network of 20,000 sensors, its BrightMail anti-spam service and 2 million "decoy" accounts around the world.

More online!

Johna Till Johnson, founder of Nemertes Research, offers practical advice in this Webcast for structuring what's called "The New Data Center."

DocFinder: 1948

PREEMPTIVE SECURITY IS HERE:

Finally, YOU CAN Chart the Difference BETWEEN INTERNET SECURITY PLATFORMS:

(A) We you from the threat here

(B) The other guys to the threat here

SAML 2.0 gets standards stamp

■ BY JOHN FONTANA

A standards body has approved the long-awaited Version 2.0 of the Security Assertion Markup Language, a milestone that is expected to add fuel to corporate interest in sharing identities with business partners.

Version 2.0 also should fan the flames around integration of SAML and competing federation protocols, most notably WS-Federation, which Microsoft and IBM developed.

SAML is the leading protocol in use today for federating identity, which lets companies issue user authentication and authorization credentials that are valid across corporate boundaries. The Organization for the Advancement of Structured Information Standards (OASIS) last week put its stamp of approval on SAML 2.0 after nearly 18 months of work.

SAML 2.0 brings together work by OASIS, the Liberty Alliance and Shibboleth, an effort to create federated identity standards for Internet2.

"SAML 2.0 is a milestone for the federation industry and will likely be a major accelerant," says Andre Duran, CEO of PingID, which develops a federation server called PingFederate. "Standards fragmentation has kept the market confused and implementation overly complicated. At this point, mainstream adoption of identity federation is no longer inhibited by standards, but by quality products which are tested secure and validated interoperable."

A group of 13 vendors met last month at the RSA Conference to prove interoperability during a SAML 2.0 test that included the federal government and its E-Authentication Initiative.

SAML already enjoys some high-profile test cases in deployments by Fidelity Investments, which has more than 200,000 end users accessing benefits information using SAML-based federation services, and at Boeing, which has nearly a dozen SAML projects underway including a federated identity project with Southwest Airlines.

SAML 2.0 is significant because it adds features such as account linking, global logout, attribute exchange with privacy features and interoperability with Shibboleth and Liberty.

While those features pump up the potential of the protocols, experts say corporations will have to perform privacy impact assessments and more deeply integrate security and directory infrastructure before rolling out SAML 2.0. Also, cross-company testing and deployment will be more complex over the basic federation offered with SAML 1.0 and 1.1.

Despite the milestone that SAML 2.0 represents, what is still missing is an intersection with work Microsoft and IBM are doing around WS-Federation. Experts say the two eventually will converge, but the effort currently appears to be stagnant.

In the interim, Microsoft's WS-Federation partner, IBM, has decided to support the trio of federation protocols, SAML 2.0, Liberty and WS-Federation, in a forthcoming version of its Tivoli Federated Identity Manager, which is currently in beta testing. Also, RSA Security and VeriSign, which helped co-author WS-Federation, plan to support Liberty and SAML. And other identity stalwarts such as Sun, Oblix and Computer Associates/Netegrity plan to support all three protocols.

Microsoft officials say they will evaluate SAML 2.0 and determine how the protocol's token format will be supported within WS-Federation.

The SAML protocol includes both a token format and a request/response engine that are tightly coupled. WS-Federation, which separates the request/response engine and token format, supports many tokens, including SAML, Kerberos and X.509.

This fall, Microsoft plans to offer its first federation server with support for WS-Federation with the release of Active Directory Federation Services. ■

Azaleos

continued from page 17

messaging. You can think about this, in the consumer space, as the TiVo of enterprise messaging."

The OneServer, which supports up to 2,500 users on one appliance, wraps Exchange and Active Directory interfaces into a set of .Net Web services that Azaleos uses to remotely access the OneServer. The appliance also features third-party software, including Sybari Antigen for Exchange 8.0 to provide anti-virus and anti-spam capabilities, Enterprise Vault from KVS for archiving and compliance and GoodLink Server technology by Good Technology to support mobile users.

OneServer also exposes the APIs that let Exchange integrate with Microsoft's other collaboration servers and tools such as Microsoft Operations Manager.

OneServer also includes directory migration tools that can pull in user information and automatically create mailboxes, an embedded SQL Server-based help desk ticketing system, role-based administration for user self-service and transaction audit logs.

Azaleos was founded in August 2004 by Microsoft veterans Roger Gerdes, who is CEO, and Keith McCall, who serves as CTO, and is backed by a Series A round of funding from Second Avenue Partners.

OneServer costs $30,000 and $35,000 with 1T byte of storage. The cost for OneStop Subscription Service starts at $7 per user, per year. ■

www.iss.net

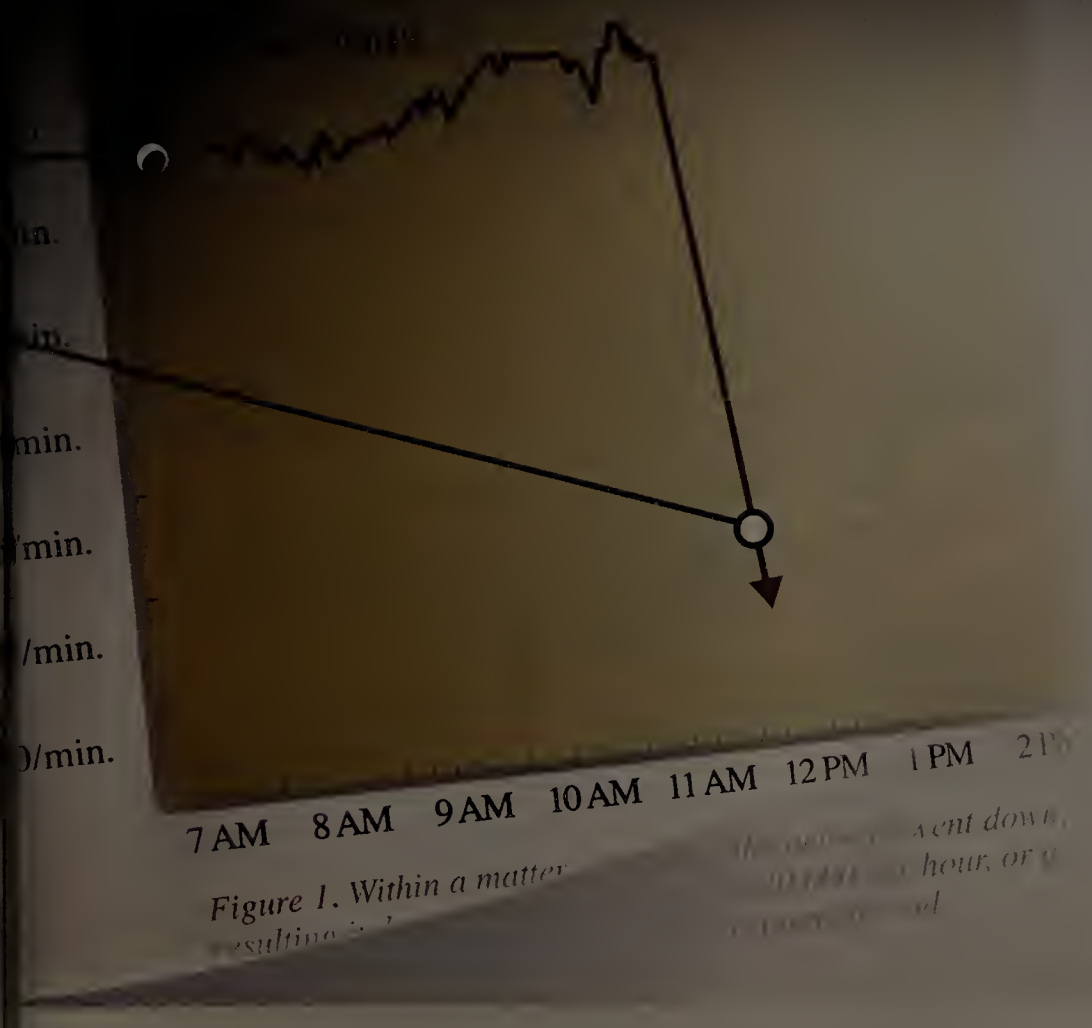


Figure 1. Within a matter

When business losses are measured in seconds, preemption beats "reaction" every time.

The only effective security is preemption. This preemptive power is only available with the Proventia™ ESP Security Platform from Internet Security Systems. When software security flaws are discovered, Internet Security Systems' world-renowned research team updates Proventia to immediately shield against any attacks targeting weak spots. Regardless of the size of your business, this new standard in Internet security can help keep you off the path to disaster and reduce your total cost of ownership – In fact, when we manage Proventia for you, we'll even guarantee protection. **Need proof? Get your free whitepaper, *Preemptive Protection: Setting a New Standard in Security*, at www.iss.net/proof/wp or call 800-776-2362.**

INTERNET | SECURITY | SYSTEMS®

Ahead of the threat.

NETWORK & HOST INTRUSION PREVENTION | VULNERABILITY MANAGEMENT | MANAGED SECURITY SERVICES

© 2004 Internet Security Systems Incorporated. All rights reserved.

Special Focus

NETWORK INFRASTRUCTURE: The Gigabit Ethernet players.

Extreme and Foundry keep on ticking

■ BY PHIL HOCHMUTH

Among the hype-fueled Gigabit Ethernet start-ups that emerged in the mid-1990s — Alteon, Granite Systems, Prominent, Packet Engines, Rapid City — Extreme Networks and Foundry Networks are the last independent vendors still standing.

Extreme CEO Gordon Stitt and Foundry CEO Bobby Johnson say the ability to adapt to market changes, innovate during downturns and push into new markets has helped their firms remain intact. Observers say each vendor still faces challenges from LAN and WAN commoditization, new low-cost competitors and the same nemesis both firms shared nine years ago: Cisco.

Both Extreme and Foundry came roaring out of start-up mode with flashy new Gigabit Ethernet switches. The companies' fortunes were taken to greater heights as the telecom and dot-com bubble swelled, with Internet companies buying up gear for speeding Web sites and carriers rolling out equipment for meeting skyrocketing bandwidth demands.

After IPOs, which flooded both companies with capital, both vendors went hard after the emerging telecom market, particularly metropolitan-area network service providers, which promised services such as Fast and Gigabit Ethernet services based on dark fiber. Both companies developed technology to let their switches act more like SONET gear in carrier networks, developing technologies that allow for fast traffic failover, QoS and security in the cloud.

Extreme's Stitt says he likes the decisions his firm has made in venturing into new markets.

"We haven't been afraid to break with our history," Stitt says, referring to forays the LAN switch company has made into wireless LANs (WLAN) and carrier network technology. "We wanted to build a long-lasting, sustainable company. [But] if Cisco was the General Motors of the industry," when Foundry came on the scene in 1996, "we wanted to be Porsche," Johnson says.

Both CEOs say that staying innovative during the technology downturn between 2000 and 2002 was key to their survival.

Stitt says two of Extreme's "biggest innovations" — its fourth-generation of ASICS and its modular XOS switch operating system — were developed between 2001 and 2003.

Likewise, Johnson says his firm is stronger coming out of the downturn.

"Those storms slowed down some of our initiatives," he says, with the vendor's revenue shifting drastically from 75% carrier/25% enterprise to the current ratio of 75% enterprise/25% carrier. "But it hasn't changed the core culture of Foundry. We did very little layoffs, and we remained profitable [through most of the downturn] and continued to hire through the majority of that time," he says.

Growth areas the CEOs foresee the extension of Ethernet into carrier networks.

"U.S. [carriers] are stubbornly sticking to SONET technologies, whereas the rest of the world is going to Ethernet," Stitt says.

"There are tremendous cost savings" yet to be realized by large U.S. carriers by using 10G Ethernet vs. OC-192 SONET technology, Johnson says.

Foundry and Extreme have had similar revenue numbers over the last several years; Extreme has averaged about $411 million in revenue per year since 2001, while Foundry's revenue has averaged $355 million. The momentum of late is with Foundry, with its sales jumping from $311 million in 2001 to $409 million last year.

Extreme has seen its sales slide from almost half a billion in 2001 to $351 million last year. Meanwhile, Extreme has posted losses the last four years, while Foundry has been profitable since 2001.

As for market share position, both firms have hovered in the same neighborhood. In 2001, Extreme had 3.3% of the total LAN switch market revenue, while Foundry's share was 2.2%. Last year, Foundry accounted for 3.2% of the total LAN switch sales, while Extreme's share was 2.2%.

Over the years, both vendors have gone after new markets with mixed results. Foundry made Layer 4-7 switching a pillar of its product offerings. Extreme purchased Web switching vendor WebStacks in 2001, but did not establish a significant presence in the Layer 4-7 market.

For Foundry, entrance into new markets remains mostly through internal product development, driven by the demands of its current customer base.

For Extreme, other areas for growth include the closer integration of enterprise software applications and the network hardware layer.

"If you look at the way the companies are run, they reflect the personality of the CEOs," says Zeus Kerravala, an analyst with The Yankee Group.

Extreme's Stitt "does a lot of public speaking and is very visible on Wall Street," Kerravala says. "Bobby [Johnson] has been much more conservative. He's been reluctant to get into markets Wall Street has advised him to get into [such as enterprise routing]. He's been very singularly focused in building a high-performance product. It's not very sexy, and Wall Street often doesn't like the approach."

The names of the two companies are also very fitting, he says.

"You think of Foundry as a bunch of guys in a hot room banging on metal. You think of Extreme, you envision guys in baggy pants saying 'Hey, dude,'" he says.

Kerravala says Foundry has been successful at sticking with its focus on high-performance.

"What they sell is very basic — a high-performance switch at a fair price. That's always been their differentiator. It was a little boring in the '90s, but they stayed with what they knew."

Meanwhile, Extreme's shifts in focus over the years might have held back the company's ability to establish itself in a particular niche.

"But if you ask people why they bought Extreme, they'd say it's because they're like Cisco, but cheaper," Kerravala says.

The challenge for both vendors is finding new ways to grow in a market that is becoming commoditized with lower margins and more competition from low-cost competitors. Both vendors have made forays into the WLAN market as a way to grow revenue from their customer bases. Foundry also has introduced WAN router/firewall products for enterprise customers, hoping to skim some market share from router leader Cisco. ■

Dealing with the ups and downs

Some high and low points of network rivals Foundry Networks and Extreme Networks since their respective beginnings.

2000
- Foundry introduces its NetIron Internet router, targeting rivals Juniper and Cisco in the 'Net core.

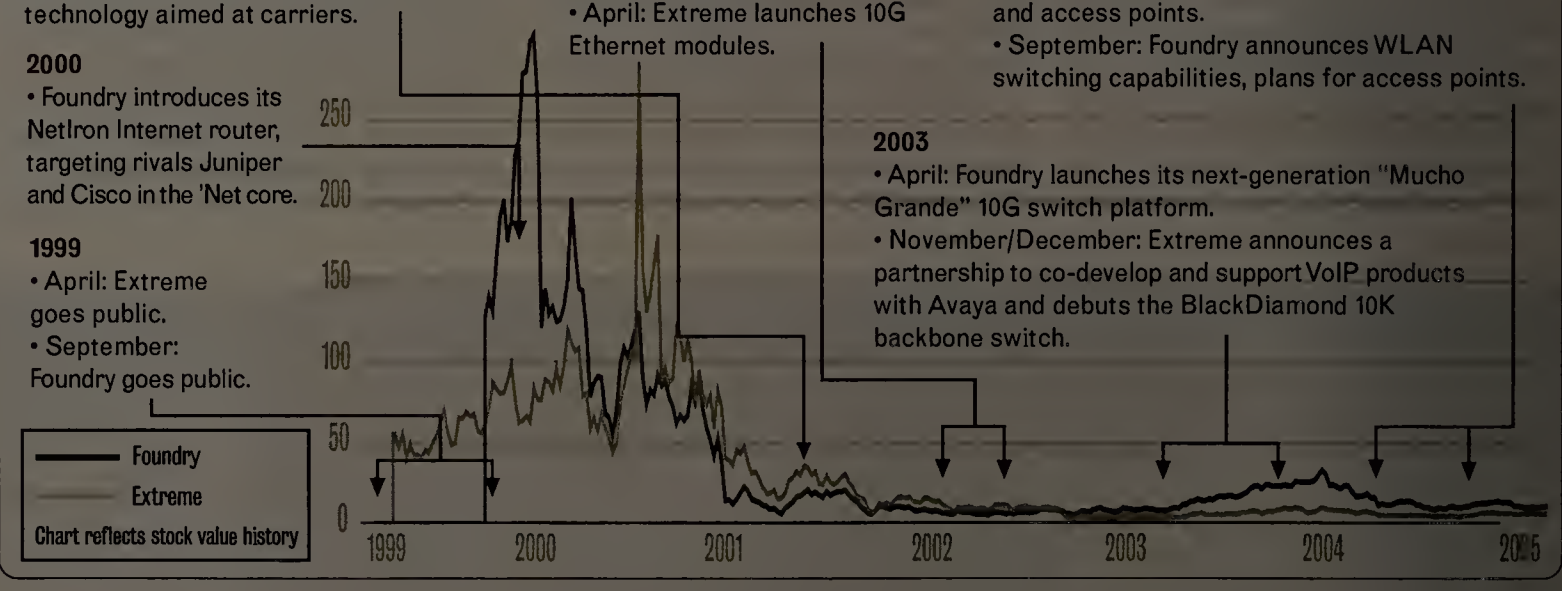
1999
- April: Extreme goes public.
- September: Foundry goes public.

2001
- Extreme introduces Ethernet Automatic Protection Switching, a SONET-like technology aimed at carriers.

2002
- January: Foundry introduces 10G Ethernet modules.
- April: Extreme launches 10G Ethernet modules.

2003
- April: Foundry launches its next-generation "Mucho Grande" 10G switch platform.
- November/December: Extreme announces a partnership to co-develop and support VoIP products with Avaya and debuts the BlackDiamond 10K backbone switch.

2004
- March: Extreme jumps into the WLAN market with its Summit S400 series of WLAN switches and access points.
- September: Foundry announces WLAN switching capabilities, plans for access points.



Your potential. Our passion.

Microsoft

BizTalk® Server 2004 named *InfoWorld's* best Process Automation Solution.

Get the story or enlist a Microsoft® Certified Partner at microsoft.com/biztalk

Microsoft Windows Server System

gy of the Year Awards," *Info* or , January 3, 2005 © 2005 Microsoft Corporation. All rights
ows Server System, and "Your po al. Our passion." are either registered
for other countries. The names of ual companies and products mentio

NETWORLD+INTEROP

LAS VEGAS • MAY 1–6, 2005

Network Insfrastructure and Services
Wireless
Security
Performance
VoIP and Collaboration
Data Management and Compliance

See it All in One Place

ALL SYSTEMS GO

350+ Top Exhibitors on the Exhibit Floor with 8 Targeted Technology Zones and Pavilions

100+ Educational Sessions, Including 6 Comprehensive Conferences Revolving Around 6 Key Themes, 3 Special Interest Days and 36 Tutorials and Workshops

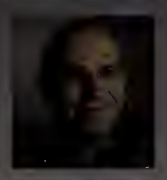
6 Visionary Keynotes by Leading Industry Executives

Survivor Las Vegas

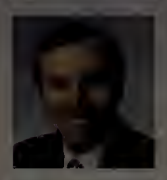
NetworkWorld Survivor Las Vegas

Visionary Keynotes

John Chambers
President and Chief Executive Officer
Cisco Systems



Hossein Eslambolchi
President—AT&T Global Networking Technology Services, Chief Technology Officer and Chief Information Officer, AT&T



Scott Kriens
Chairman and Chief Executive Officer, Juniper Networks

Sean Maloney
Executive Vice President General Manager, Mobility Group, Intel

Andy Mattes
President and Chief Executive Officer, Siemens Communication Networks

Your Source for Building a Better IT Infrastructure

MediaLive INTERNATIONAL

Copyright © 2005 MediaLive International, Inc., 795 Folsom Street, 6th Floor, San Francisco, CA 94107. All Rights Reserved. MediaLive International, NetWorld, Interop and associated design marks and logos are trademarks or service marks owned or used under license by MediaLive International, Inc., and may be registered in the United States and other countries. Other names mentioned may be trademarks or service marks of their respective owners.

Register Today at www.interop.com

Use priority code MLAHNV01 and receive $100 off any educational product.

NetworkWorld Perspectives

March 21, 2005 | Insights on key issues facing network IT

LOCKING DOWN APPS

Because perimeter security will never be perfect, experts turn their attention to securing the corporate jewels — the applications.

■ *By Joanne Cummings*

Your organization understands security. It follows best practices, has the requisite firewalls, anti-virus and intrusion-detection systems in place along the perimeter, and only communicates with mobile users or business partners via secure VPNs.

And when end users enter the network via the VPN they are vetted by a separate security server to ensure their machines are properly configured with the appropriate firewall and anti-virus tools before they're granted access to core applications.

The company even goes as far as deploying application-specific firewalls and intrusion-prevention systems (IPS) around the most critical application servers, watching for and blocking non-appropriate application calls and traffic. It's what the pundits call "defense in depth," and you've got it in spades.

But even though the company has probably spent thousands, maybe millions, of dollars on security infrastructure, chances are it will still get hit by the latest virus or worm.

"What's wrong with this picture?" asks Paul Simmonds, director of global information security at London chemical conglomerate ICI and a co-founder of the Jericho Forum. "What we have is back to front, at the moment. We're saying that since we can't secure our applications, we need to put in firewalls and kludges all over the place to make what we have at least semi-secure, and even that's not working. But why not just go back to first principles and get this secure from the outset, at the application level?"

An applications deployment nightmare

Experts agree that the security focus needs to shift. "For anybody who's thinking about new hacking techniques, the soft target now isn't the network or the operating system. It's the applications," says Thomas Longstaff, deputy director for technology at security organization CERT. Because no matter how much technology you put in place around applications, in order to use them, you have to open them to end users and other processes.

"It doesn't make any sense to protect all this information if you can't get to it," Longstaff says. "You have to provide access to wherever the clients happen to be. And that means that you're really relying on the proper configuration and security of not only every application server but also every end user that's going to use the application."

Complicating matters is that application vendors implement security measures differently such as authentication and authorization, encryption and so on.

ILLUSTRATIONS GIACOMO MARCHESI

"We're still pretty much in the Wild West phase of applications security, where everybody who has a good idea goes off and does it their own way," Longstaff says. "Very few vendors are trying to bring their applications together under a single framework for security."

That makes it hard for end users to securely deploy and configure their business-critical applications. "When deploying new applications, users are faced with a long list of security check boxes," Longstaff says. "And the onus is on them to figure out each application's inherent security problems, how best to shore them up, and then how to make sure the best security configurations for one application don't interfere or override the security configurations for another."

That's now the most daunting area, says Brian Young, vice president of IT at Creighton University in Omaha, Neb. "It's like you have to be a NASA engineer to make the security pieces work for some applications," he says. "In many cases, the only folks who know how to work it are the engineers in the company who built it. And that's not user-friendly. It makes it really difficult to deploy."

Longstaff says applications vendors will eventually have to rally around standardization, some kind of security middleware that will ensure that every application implements security in a standard way.

"When we have a better layer of middleware out there that the applications developers can begin to use, then this problem will get better," he says. "We will have tighter application security, a more uniform interface and an easier end-user experience when adjusting the security parameters."

But all that will take time, and while the industry waits, applications will continue to be soft targets.

Interim solutions

That doesn't mean today's organizations can't keep their applications secure. Experts say the key is to deploy applications-based security strategically, with an eye to the future. Many organizations looking at applications security tend to focus on IP-based solutions such as application-specific firewalls or IPSs. Proponents of these tools tout the fact that they can be deployed around critical applications servers and then outfitted with policies to ensure that only acceptable types of traffic can access the application.

"Rather than identifying and blocking all the bad traffic, we take it from the other perspective and say what traffic should be allowed, what is acceptable to the application," says Mike Paquette, vice president of marketing and product management at IPS vendor Top Layer Networks. Paquette says tools like his firm's Attack Mitigator can shore up application defenses, especially in cases where the applications haven't been configured properly for security.

Say you roll out a Microsoft Web server and enable WebDAV, a Web authoring tool that shouldn't be turned on in a production environment. "It's a mistake," Paquette says, "but you can set up a policy within an IPS to watch every request that comes into that application, and if one contains a command specific to WebDAV, you can block it." It's an added layer of protection.

Such tools are helpful but don't solve the right problem in the long run, some experts say. "You really need to move up the stack," says Andreas Antonopoulos, senior vice president and founding partner at Nemertes Research. "Using a firewall or IPS that can understand TCP or HTTP isn't really the right way to do it. You're peeking up into the application from the network layer, but you're still very much tied to the IP address, and you're still very much grounded in the network."

Such an IP-centric strategy becomes es-

5 steps to strong application security

1. Take application security as seriously as network and operating system security. Many organizations have bulletproof policies around operating system patch management and network configuration management but have no policies concerning upgrading application security and configurations. But applications are just as important, if not more so, when building good security postures.

2. Purchase with application security in mind. Not only should you stipulate good application security, but users should require ease of use and interoperability within their applications contracts.

3. Don't tie security to the network. As networks and data centers evolve, the best security will be at the application layer, within the protocols, and not tied to IP addresses.

4. Keep an eye on Web services and identity management. These areas currently are pursuing the best models for ensuring application-level security.

5. Be proactive. At the least, insist that every new application you buy supports secure protocols and doesn't rely on lowest common denominators such as FTP and Telnet.

pecially problematic when firms begin moving to the concept of the new data center, in which core applications servers are virtualized and applications are provisioned automatically and on demand. Using IP-based security tools in such a flexible environment leads to unnecessary complexity and can hamper the organization's ability to do business.

"You end up tying your infrastructure down and making it less dynamic," Antonopoulos says.

This is because such tools tend to associate specific servers at specific IP addresses with specific functions, such as Web serving.

"And that totally negates the idea of any automated provisioning system," he says. "In that scenario, you have two choices: Either your security infrastructure becomes more flexible and adaptive, or you're forced to set up a ton of proxies and redirections and things like that to compensate."

Instead of using the IP address for a Web server, organizations should set up things like DNS to resolve the IP addresses dynamically as they move applications on the fly, he says. "But that's terribly kludgy," he says. "For one thing, you've introduced a security risk so that if someone rewrites that DNS entry, they can hijack your Web server. And secondly, you've added another layer of redirection, which is a nightmare."

The best approach, Antonopoulos says, is identity management-based security. "With identity management, you ignore the network completely," he says. "So instead of thinking of the finance department as five IP addresses, it becomes five servers or users. It's all policy-based, with application domains and organizational domains within the company that are completely disassociated from the underlying network."

He also says emerging protocols, such as the Security Assertion Markup Language (SAML), which lets Web services applications exchange authentication information at the middleware layer, are a step in the right direction.

"That stuff is available now, but it's only happening among the vendors who see it from the application perspective," he says, adding that the vendors to watch are in the identity-management and Web services realms. "If they support SAML today, they get it."

Proactive steps

In the end, the best defense is always a good offense. Rather than complacently accepting unsecure applications, experts urge companies to demand better application-level security from the vendors.

Creighton's Young says he avoids security configuration and interoperability problems by making key stipulations in applications contracts.

"Before we sign a contract to buy an application, I add in clauses for service-level agreements and assurances that the applications' security levels are both easy to configure and as user-friendly as they were said to be," Young says. "And if there are conflicting issues between applications, I say it's their problem and they have to bring about a resolution. We wrap all that into the contract, and it lets us turn the tables on the vendors and make them accountable."

Similarly, it's important to demand that applications vendors support secure protocols. ICI's Simmonds says his business units are continuously pressuring him to make it easier to run applications over the Internet, for flexibility and cost. "But the Internet fundamentally is insecure," he says. "And you'd be surprised, but a lot of vendors don't seem to realize that. They still design new applications that use Telnet and FTP."

One ICI business refused to accept FTP as the default standard in an ERP application. "We told our ERP vendor we were required to use AS2 to communicate with our business partners and asked them how to go about it," Simmonds says. Little did ICI know, but the vendor already had an AS2 plug-in module available. "We bought the module, plugged it in and a week later, we were up and running."

"This stuff is possible, and it does exist," he says. "It's just that it's a secret and the default — the accepted way that they tell you to do it — is to use FTP, which is wrong."

Simmonds says users should demand that application-level security work within your company as well as across companies, customers and business partners.

"Today, Microsoft will say if you buy our latest Office suite and XP, you can do secure digital encryption and management on all your documents," Simmonds says. "But if you need to do business with a partner on Unix or running an earlier release of Office, it won't work. Either you don't do it, or you have to decrypt it when it goes outside your business. That's not acceptable."

The key, he says, is to spend less time evaluating and managing interim solutions and more time pushing vendors to shore up applications.

"The danger is that we're so caught up in all of these wonderful initiatives and the latest black box that we lose sight of the big picture," he says. "You have to put in these things now because your business still needs to run. But what you need to do is save 15% to 20% of your time to step back and realign your resources to where they'll do the most good — on the applications end."

> "YOU NEED TO SAVE 15% TO 20% OF YOUR TIME TO STEP BACK AND REALIGN YOUR RESOURCES TO WHERE THEY'LL DO THE MOST GOOD — ON THE APPLICATIONS END." **Paul Simmonds, ICI**

In the rosiest scenario, vendors eventually will produce applications that can run securely over the Internet, without the need for savvy customers implementing the appropriate security via firewalls, VPNs and other devices ad nauseum.

But if that scenario is to approach reality, organizations need to start prodding vendors now. "You have to remember that anything you are getting on the market in two year's time is in the R&D lab today. So we need to influence that now," Simmonds says.

Cummings is a freelancer in North Andover, Mass. She can be reached at jocummings@comcast.net.

2:07PM LOG IN TO HOT SPOT 2:08PM NETWORK SECURES THIN AIR 2:09PM TRANSMIT FILES THROUGH THIN AIR 2:25PM UPDATE PURCHASE ORDER 2:35PM EXPENSE COFFEE ORDER

The more freedom you give employees to work anywhere, the more you can achieve. That's good. But, at the same time, the more you expose yourself to intruders and worms. That's not so good. How far can a network travel to protect your office? Now, the answer is everywhere. Cisco networks, with integrated wireless security, protect mobile workers who constantly move outside the safety of the corporate network. So information is secured. No matter where it exists. To learn more about how Cisco can help plan, design and implement your network security, visit cisco.com/securitynow. **SELF-DEFENDING NETWORKS PROTECT AGAINST HUMAN NATURE.**

Cisco Systems

THIS IS THE POWER OF THE NETWORK. NOW.

©2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, Cisco IOS, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

Enterprise Computing

■ WINDOWS ■ LINUX ■ SERVERS
■ STORAGE ■ GRID/UTILITY ■ MOBILE COMPUTING

In Site: Lessons from leading users

Grid technology aids hospital's diagnostics

■ BY DENISE DUBIE

Doctors often need to balance the urgency of medical conditions with performing thorough analysis to arrive at an accurate diagnosis. Ideally, they'd like to do both.

Dr. Eric Bremer at Children's Memorial Research Center in Chicago turned to data mining and grid technology to help his organization garner speedy research results, while also performing thorough analysis. With nearly 3,000 children diagnosed with brain tumors in the U.S. each year and more than 12 brain tumor types, he says it's critical that doctors hit the right diagnosis — fast.

Using grid technology, the hospital's director of the Brain Tumor Research Program was able to reduce the time it took a text-mining application to run from more than 24 hours to just less than an hour and 20 minutes. Aside from tapping internal resources, Bremer says he expanded his research capabilities and speeded results without adding significant cost, maintenance and IT burdens.

"Our overall goal is to define better diagnostics and therapies for kids with brain tumors. We wanted to lift the human barrier to working with such vast amounts of data within realistic time frames," he says.

Bremer last year rolled out LexiQuest Mine, a data-mining application from SPSS, to start pulling relevant information out of 125,000 document abstracts from 21 medical journals. With more than five years of research at his fingertips, he says he thought LexiQuest Mine would help him more quickly classify brain tumors in patients.

The software lets researchers ask questions, extract concepts and relate the analysis to known brain tumor diagnosis criteria such as gene lists. LexiQuest Mine helped the doctor query and retrieve documents, but more importantly mine the text for concepts. For example, the analytics software understands how groups of words work together such as clinical trial vs. failed clinical trial. Text mining would deliver more accurate results than, say, a search program.

The problem with the software is that it took more than a day to generate some results.

"Initially, I thought the application had shut down, but that is just how long it took to process the request from a workstation," he says. "I quickly realized it wasn't humanly possible, even with this application, to realistically mine the amount of data I needed to mine for research."

Bremer then considered whether other technology could help advance his scientific endeavor.

"I am not an IT professional, but I was familiar with the notion of high-throughput and high-performance computing options," he says.

He considered grid computing an alternative to investing in high-end servers. Because of cost, space and potential managerial constraints, he wanted to better use the computing power he had in-house.

With the help of SPSS, Bremer became acquainted with grid computing products from United Devices. The application provider wanted to ensure its software met the specifications the doctor required and offered to grid-enable the application. SPSS had been a node on United Devices' worldwide grid since 2001.

"The application has different modes in which it can run, and each mode has a process that is a series of steps, and each step has a wrapper around it. The grid technology can grab the wrapped step and send it to any idle processors on the grid," explains Catherine DeSesa, system engineer at SPSS. "Most applications that use command-line scripts can be grid-enabled."

Working with professional services folks from SPSS and United Devices, Children's Memorial rolled out its pilot of United Devices' GridMP Workstation product in October.

The software consists of a central Linux-based server and agents distributed to Windows machines designated to be on the grid. The software taps unused and idle processor time on doctors' and researchers' desktops and laptop computers. Upon a user request, the server software will parse out parts of the LexiQuest Mine application process to available machines. The machines perform their part of the job and return the results to the GridMP Server, which recompiles the data and delivers it to the user via a Web interface.

Policies defined in the software determine which machines can be used and eliminate the need for the researcher to assign the jobs to machines. Yet the grid has its limitations. It's restricted to internal PCs because of firewall and licensing issues, Bremer says.

Bremer started with about 18 desktops, expanded the pilot to more than 25 end-user machines and plans to increase it to more than 100 in the next few months.

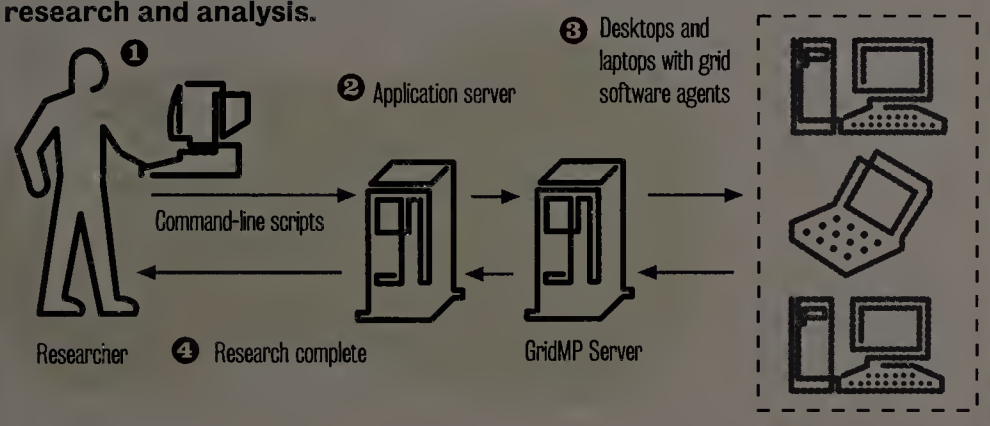
"We get through a lot more data a lot more efficiently now," he says. His team was able to define data-mining workflows and automate about 80% of the process with the grid in place. Bremer's not sure the other 20% needs to be automated and plans to expand its use to more applications.

"The best result of the grid is that it opened our eyes to a lot more ways we could use it," he says. "We lifted a barrier to being able to do more computationally intensive experiments."

While Bremer did not discuss specifically what his organization spent on the grid software, he says he was able to use an existing Linux server. United Devices says its GridMP Workstation product can start at $50,000 and scale according to the number of servers, agents and additional components purchased. Pricing for LexiQuest Mine starts at $60,000. ■

Divide and conquer

Children's Memorial Research Center uses grid technology to split the processing load of a text-mining application among desktops and laptops and is able to get speedier results to further pediatric brain tumor research and analysis.



1. A researcher uses a Web interface to begin a text-mining application process on the application server. The researcher specifies the data to be found in more than 124,000 medical documents, how it should be presented and who should receive it.
2. Application server sends the job to the GridMP Server, which searches the grid of desktops and laptops for idle processors, parses the text-mining application based on available machines and distributes the job to end-user devices equipped with agent software.
3. The desktops and laptops in the research center's grid process their part of the job and send the text mining results to the GridMP Server.
4. The GridMP Server waits until all processing is done, accepts completed jobs from grid machines, recompiles the parts of the text-mining application according to the researcher's earlier presentation request and delivers the results via the application server to a Web interface.

WIRED WINDOWS
Dave Kearns

Microsoft getting Active Directory right

I spoke with Microsoft's Stuart Kwan and Kim Cameron last week at NetPro's Directory Experts Conference. Kwan is the director of program management for identity and access in the Windows Server group, while Cameron is identified as "identity architect" — that means eminence grise, or the guy Kwan can blame for the really bad ideas.

The important message I got was that (finally) Microsoft was taking identity — and Active Directory — seriously. Well, the company is taking Identity and Access Management seriously, and to do that it needs to give priority and prominence to Active Directory. It's a far cry from 1999 when Active Directory was often considered an evil — albeit a necessary evil — adjunct to the server operating system. Users drove the change in priorities because they demanded better facilities to support federated services, regulatory compliance, electronic provisioning and more — all of which rely on the directory as platform.

The duo outlined the road map for the directory going forward. First, in the upcoming R2 release of Windows 2003 Server there will be schema extensions in support of Unix and Linux compatibility. Yes, Microsoft is admitting that you might have some non-Windows platforms in your network mix! The new extensions will facilitate third parties (such as Vintela and Centrify) that provide authentication services to non-Windows platforms but have run into some resistance from users not wishing to do ad hoc schema extensions.

There are big plans for the next release of Windows server (code named Longhorn), including the concept of Read-Only domain controllers (all the best parts of the old back-up domain controller without the headaches). Because Longhorn also will allow you granular control of the services running (including such anomalies as a command-line driven Windows server), you'll be able to build a minimalist domain controller with few other services running thus minimizing the security holes that might be available.

Two huge gains for IT and ID managers to come in the Longhorn release are the ability to differentiate between Domain Administrators and Domain Controller Administrators (for much better security), and a resetable Active Directory to minimize the number of required re-boots. Increased security and less downtime are two good reasons to look forward to Longhorn.

Active Directory finally is taking its rightful place as the platform for all sorts of services in the realm of identity management. It finally might be fulfilling its promise.

Kearns, a former network administrator, is a freelance writer and consultant in Silicon Valley. He can be reached at wired@vquill.com.

Tip of the Week

I'll be saying a lot more about Active Directory, DEC, Kwan and Cameron in this week's **Identity and Windows networking newsletters,** make sure you're subscribed. If not, head to www.nwwsubscribe.com and sign up now.

More online!

Get an insider's understanding of the technological advances that are below the radar of most WAN watchers. Attend a new Network World Live '05 Technology Tour Event that delivers new tools and real-world solutions.

DocFinder: 6235

The most secure console & terminal server management solutions in the industry!

Solaris Ready
RSA SECURED

Formerly XYPLEX

• More ports shipped than all of our competitors combined!

• Over 20 years of experience in the industry!

• The best security with per port password protection, RADIUS, Secure Shell v2.0, SNMP V3, SecurID, TACACS+, PPP PAP/CHAP, PPP dial-back, on-board data-base and more!

• Integrated secure power management allows direct power control.

• Global certifications, including NEBS Level 3.

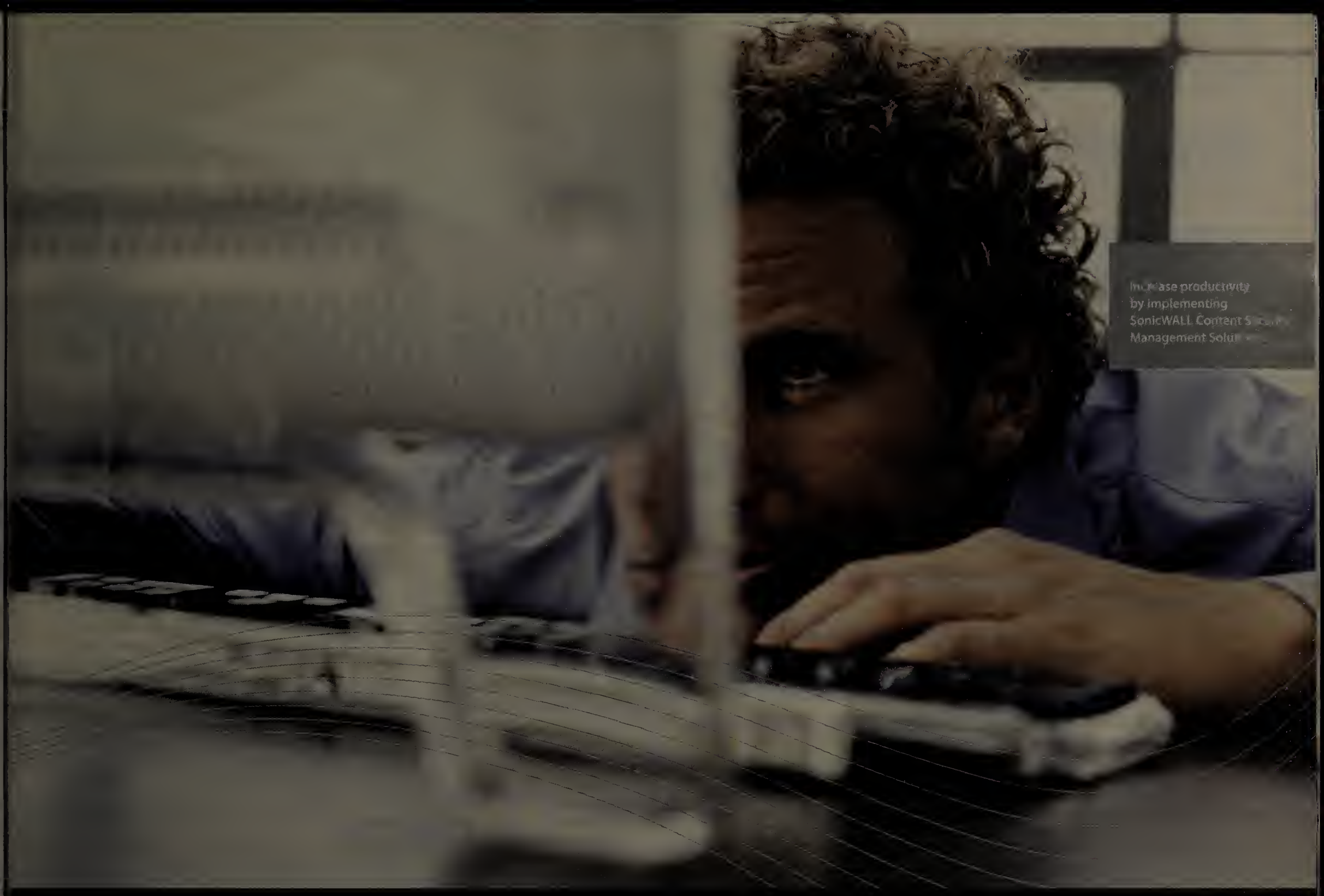
• The largest range of products in the industry! (optional optical uplinks available)

MRV console servers offer a highly-reliable, easy to manage rich set of features, making secure remote management of IT assets possible from any location.

please visit us at

or call us at

MRV



It's 10am. Do you know where your employees are?

The reality could be quite costly.

But how can you install enterprise-class content management technology, without spending mountains of cash? The answer is SonicWALL®. We take state-of-the-art network security and make it simple, affordable and reliable. So businesses like yours can stay focused on business.

Using a dynamic, real-time rating architecture and a comprehensive database of sites and domains, our Content Security Management Solutions give you total control over Internet access. You can easily set times for accessing shopping, banking and other personal Web surfing sites. And advanced analysis and reporting give real insight into network usage. All in one affordable, usable package. That's the SonicWALL way.

Stop wondering where your employees are. For more details on our SonicWALL Content Security Management Solutions, visit **www.sonicwall.com/csm** or call us at 1.888.557.6642.

Around the clock, around the world, and around the Web–
SonicWALL is there for you.

SONICWALL

Anti Virus ▪ Anti Spyware ▪ Intrusion Prevention ▪ Content Security ▪ Secure Wireless ▪ Firewall ▪ VPN

COMPLIMENTARY EVENT
FOR PROFESSIONALS ONLY

NetworkWorld® LIVE 05
TECHNOLOGY TOUR AND EXPO

THIS EVENT IS COMING TO A CITY NEAR YOU

DALLAS, TX | April 5, 2005 SAN FRANCISCO, CA | April 7, 2005
WASHINGTON, DC | April 12, 2005 NEW YORK, NY | April 14, 2005

Remote Office Networking:

Bringing the Enterprise Together

Join James Gaskin, Principal, Gaskin Computer Services, and leading solution partners for this Network World Technology Tour and Expo

Remote Office Networking shows you how to satisfy your enterprise's seemingly conflicting demands for remote office networking without sacrificing control; flexibility as well as protection from hackers; more user productivity while lowering costs for supporting far-flung workgroups. You'll get immediate-impact ideas, information and options that will reduce your remote office costs, increase your core security, and maximize your management efficiency. All while building an integrated remote office network that unites your enterprise.

PRESENTING SPONSORS

3Com
Exercise Choice™

3Com is a leading provider of secure, converged voice and data networking products and solutions that improve business value for enterprises of all sizes. More than any other company, 3Com brings the power of choice to enterprise customers.

ADTRAN

ADTRAN's NetVanta solutions are designed for cost-effective branch office connectivity and include routers; managed Fast Ethernet, Gigabit, and PoE switches; VPN/firewall devices and an industry first - one product that combines a managed 24-port Ethernet switch, router with WAN interface, and firewall, with options for VPN and PoE, all in a single 1U chassis.

INTERNET|SECURITY|SYSTEMS®
Ahead of the threat.

Internet Security Systems (ISS) is the only company to provide truly pre-emptive protection that shields vulnerabilities and blocks attacks before they disrupt business operations. ISS delivers proven cost efficiencies and reduces regulatory and business risk for over 12,000 customers worldwide.

RIVERBED

Riverbed optimizes applications for wide area networks by addressing the two key factors that slow performance: high latency and limited bandwidth. Riverbed appliances accelerate applications up to 100 times and expand bandwidth ten-fold, enabling site consolidation of distributed infrastructure without degrading performance.

EXHIBITING SPONSORS

cyclades
K logix
A WEBSENSE PARTNER
netopia
Raritan.
When you're ready to take control.™
softwaremedium
A WEBSENSE PARTNER
TelePacific COMMUNICATIONS

Remote Office Networking: Bringing the Enterprise Together

Register now at www.nwfusion.com/RONS5A1
or call Dori Smith at 800-643-4668

To join sponsors of this premier Network World Event, or to find out more about onsite company training, please contact Andrea D'Amato at 1-508-490-6520 or adamato@nww.com for free, no-obligation information

Application Services

■ CRM ■ MESSAGING/COLLABORATION ■ WEB SERVICES
■ ERP ■ E-COM ■ NETWORK AND SYSTEMS MANAGEMENT

Offsite security complicates compliance

■ BY ANN BEDNARZ

Offsite security conditions are always a factor to consider when a company enters an outsourcing deal, but regulatory initiatives are raising the stakes.

IT executives need to ensure service providers have proper system controls in place before and after they enter into sourcing and hosting arrangements, analysts say. It's not only a good business practice, it's also increasingly required by law.

One law putting a spotlight on outsourcing deals is the Sarbanes-Oxley (SOX) Act of 2002, which Congress passed in the wake of accounting scandals at firms such as Enron and WorldCom.

SOX has IT and finance departments working closely to review and modernize companies' financial reporting systems to comply with its regulations. Of particular concern is Section 404 of the legislation, which calls for company executives and third-party auditors to certify the effectiveness of internal controls — technologies and processes put in place to preserve the integrity of financial reports.

Doing due diligence to Section 404 means looking into conditions at outsourcing and hosting providers' sites, where sensitive corporate data might be accessible, processed or stored. That's where Statement on Auditing Standards (SAS) 70 comes in.

SAS 70 is an auditing standard developed by the American Institute of Certified Public Accountants for service organizations. It prescribes a method for an auditor to examine control activities at a service organization or outsourcing firm.

There are two types of SAS 70 audits. A Type 1 audit focuses on general controls at a single point in time and doesn't include testing by auditors. A Type 2 audit is more intensive — and more appropriate for SOX compliance. It looks at conditions over a prolonged period of time, and auditors perform testing to verify the effectiveness of controls at service organizations.

SOX compliance efforts have elevated interest in the auditing standard, which has been around since 1992. "We are doing a lot more SAS 70s lately," says Ed Byers, a principal at Deloitte & Touche.

Outsourcers agree that users are beginning to ask for SAS 70 audits. "It was something our customers were looking for," says John Engates, CTO at Rackspace Managed Hosting.

Ernst & Young recently concluded an SAS 70 Type 2 audit for the San Antonio managed hosting provider. The audit covered controls related to service delivery and operations, infrastructure maintenance, change management, back-up processes, and logical and physical data center access, Engates says.

Rackspace underwent the audit at the request of some of its largest customers, which are facing SOX Section 404 deadlines, Engates says. Section 404 says companies must prepare reports — to accompany their annual reports filed with the Securities and Exchange Commission — assessing the effectiveness of their internal control structures and financial reporting procedures. Section 404 deadlines are staggered and begin this spring.

"They really need some assurance that the controls that are in place outside of the walls of their companies are as effective as the controls inside their companies," he says.

At the same time, Rackspace benefits from having gone through a formal process to analyze and document its internal controls. "It put a spotlight on our documentation and the formalization of our policies and processes," Engates says.

Securing SAS 70 certification requires a commitment — of personnel and budgets — on the outsourcing providers' part. At Rackspace, the certification process took almost one year, from the early stages of defining the scope of the audit to the full-blown testing of controls.

Sierra Atlantic will spend about $25,000 to achieve SAS 70 certification this year, says Marc Hebert, executive vice president at the Fremont, Calif., company, which offers a range of offshore application services. Sierra Atlantic is in the process of securing SAS 70 Type 2 certification.

See SAS 70, page 28

Auditing outsourcers

SAS 70 audits have been around for awhile, but they're getting closer scrutiny as public companies look to comply with Sarbanes-Oxley (SOX) requirements.

What it is: SAS 70 is an auditing standard developed by the American Institute of Certified Public Accountants to examine the system and security controls in place at a service organization or outsourcer.

Who gets one: Service organizations can request an SAS 70 audit, which an accounting firm performs.

Points to be aware of:

- SAS 70 audits don't happen overnight. It can take several months for an outsourcer to go through the process of defining the scope of an SAS 70 audit and submitting to testing by an auditor.
- There's no set criteria for testing in an SAS 70 audit. The outsourcer and auditing firm define the parameters of the SAS 70 audit, which can vary from firm to firm.
- Securing SAS 70 audits from outsourcers might not be adequate for SOX compliance. The SAS 70 auditing standard predates SOX and might not cover all the controls that SOX addresses.
- Additional documentation might be required. Companies concerned SAS 70 audits from their outsourcers aren't sufficient might need to send their own internal and third-party auditors to verify in-place processes and physical conditions at their outsourcers' sites are adequately secure.

Short Takes

■ **IBM** last week agreed to buy data integration software maker **Ascential Software** for about $1.1 billion. Ascential's products are used to build data warehouses, feed data into business intelligence systems and consolidate enterprise applications, among other things. If approved, the acquisition will strengthen IBM's information integration offerings, the company says. After the proposed acquisition, the Westboro, Mass., company would become a business unit within IBM's Information Management software division. Ascential's products would become part of IBM's software offerings and sold through IBM's and Ascential's sales channels and partners. The Ascential Enterprise Integration Suite complements IBM's WebSphere Information Integrator products, according to IBM. Ascential has more than 3,000 customers. IBM and Ascential have more than 550 joint customers.

Microsoft rolls out business app plan

■ BY JOHN FONTANA

Microsoft has taken another crack at evolving its business applications, and this means that corporations could have a more flexible upgrade path as the vendor tries to integrate its wares over the next three years and keep pace with rivals.

The news for corporate users is they won't have to rip and replace their current Microsoft Business Solutions applications — Axapta, Great Plains, Navision, Solomon and Microsoft CRM. Instead, they will see a series of upgrades that will introduce common features across the platform, including interface design, development tools; and integration points such as SQL Server, SharePoint Portal Server, Office and Longhorn.

Microsoft recently unveiled its new road map at its Convergence 2005 conference in San Diego.

As part of the plan, Microsoft also extended support for business applications from three years to five so users can stay on a given version longer before upgrading.

Experts say Microsoft's plan is twofold: One is to address user migration concerns, and the other is to catch up to rivals in the

See Microsoft, page 28

'NET INSIDER

Scott Bradner

Just doing its job

In mid-March, the George Washington University-based National Security Archive (www.gwu.edu/~nsarchiv) added to its already impressive collection of National Security Agency-related documents. The most recent addition is the December 2000 "Transition 2001" document provided to the then-incoming Bush administration. This document recommends that the agency get even deeper into the network monitoring business and makes for quite interesting reading, particularly since it is reasonable to assume that equivalent documents were created by intelligence agencies in other parts of the world.

The documents in the archive cover many issues, which include the full history of the National Security Agency and extend from 1950 to 2002 (www.nwfusion.com, DocFinder: 6329). As you might expect, Transition 2001 (DocFinder: 6330) has been redacted, but far less than I would have expected. (By the way, the National Security Agency, at least, has learned from the work of Claire Whelan — redacting is now done with white boxes that overlap the text (see DocFinder: 6331). It's fun to speculate that if the National Security Agency took the opportunity of having to produce this document to redact selectively to make some points, for example, clarifying that it has lost employees at a time when it wants more responsibility.

A few major points in the document:

- The agency is ready to deal with the explosion in global communications but to do so "demands a policy recognition that NSA will be a legal but also a powerful and permanent presence on a global telecommunications infrastructure where protected American communications and targeted adversary communications will coexist."
- The National Security Agency must "live on the network" to deal with the new world of wireless- and fiber-based data communications networks but "the NSA can perform its missions consistent with the Fourth Amendment [of the U.S. Constitution] and all applicable laws."
- The agency's mission "means seeking out information on the Global Net, using all available access techniques, breaking often-strong encryption ..."
- The new telecom world leaves U.S. networks, both public and private sector, vulnerable. But the document doesn't spend all that much time discussing this. The document also mentions that the National Security Agency suffered a three-and-a-half-day network outage in January 2000, hardly something I expected to read here (unless it already had been reported — if so, I missed it).

It might not be entirely coincidental that the National Security Agency in mid-February leaked the fact that the Bush administration is thinking of making the agency just the kind-of "traffic cop" that it asked to be in Transition 2001 (DocFinder: 6332). It sure would be good to get someone in government to pay attention to the security of government agencies, considering they were judged to deserve no better than a D+ last year (DocFinder: 6333).

Maybe the National Security Agency can help (see www.nwfusion.com, DocFinder: 6334). For now, I'll take it at face value that the National Security Agency will take pains to adhere to the law and that the laws that the agency pays attention are the laws we know about. (But I will note that the face of the agency is not all that clear.)

I assume that most other major countries have similar plans, but might lack a Freedom of Information Act to make that fact known. So maybe it's time to start protecting communications that you or your company would rather not have become general knowledge in world government circles, and maybe also in industry circles with good government contacts. Take a look at the technology at www.gnupg.org, which I've been told is what organizations like the National Security Agency use in house to foil competitors in its line of business.

Disclaimer: Foiling competitors in the higher-ed business means being better, not stealthier. Harvard hasn't expressed a view on the National Security Agency's self-opinion, and the above is mine.

Bradner is a consultant with Harvard University's University Information System. He can be reached at sob@sobco.com.

Microsoft

continued from page 27

developing Web services world.

Microsoft's original upgrade plan, dubbed Project Green, would have been a replacement for current applications, but the company is replacing the glitz of that makeover with a more pragmatic plan, analysts say. The company also has abandoned its boastful prediction from just more than a year ago that it would grow its Business Solutions Group to $10 billion in revenue by 2011.

"Project Green shook up partners and customers pretty seriously," says Chris Alliegro, an analyst at Directions on Microsoft. "If you had made investments in existing product lines, you were looking at potentially an uncertain future. You ask, 'Can I move to new products or am I looking at a costly data migration process?'"

Microsoft's plan now is to build common elements between applications such as developing 50 role-based templates for creating stock interfaces for specific users such as shipping clerks or procurement managers. The plan also is to integrate common portal technology based on SharePoint Portal Server, add support for SQL Server Reporting Services, and ship in 2006 a common user interface that incorporates similar navigation, buttons and forms.

In addition, Microsoft says it plans to create a common Web services layer based on technology it is developing in Longhorn called Indigo that will let users expose the business logic from Microsoft business applications as services within a service-oriented architecture (SOA).

Those features will be part of what Microsoft is calling Wave One of Project Green.

"The thing that they can do is bring forward what they call the user experiences," says Joshua Greenbaum, of Enterprise Applications Consulting. "They can use the extraordinary familiarity that the world has with Office and Outlook and drive a lot of functionality through that user experience. That is something, when you look at the synergy that the Business Solutions Group can have with the rest of Microsoft, that really is extraordinary, and that is where the potential gets mind-boggling."

Of course, Microsoft isn't the only one with that idea. Rivals, such as SAP, are looking to bring Office and Outlook to the front end of their platforms.

In Wave Two, which is scheduled to begin in 2008, Microsoft plans to add modeling tools for developers to map out a company's business processes and workflows, and adapt the business-logic Web services to those models.

Some experts say the rivals are fueling Microsoft's strategy change.

"There is a heightened sense within Microsoft that the real competition going forward is SAP and Oracle and to a lesser extent IBM," says Bruce Richardson, senior vice president of research at AMR Research. "When Microsoft hears about SAP building open business-process platforms or hears about Oracle's Project Fusion, they realize they need to get a bit more aggressive on the marketing side and talk about their plans for SOAs.

Microsoft officials say the change in Project Green merely reflects the hope of arriving at its goals without tearing up the entire road that's already been laid down. ■

SAS 70

continued from page 27

Like Rackspace, Sierra Atlantic decided to pursue SAS 70 certification because of customer demand, Hebert says.

In general, there's a tendency for companies to secure more SAS 70 certifications from outsourcers than are needed, Byers says. "Companies are so scared about Sarbanes-Oxley they want to audit everything," he says.

There's confusion over when an SAS 70 audit is required and when it isn't — particularly when it comes to smaller service providers that might not have the necessary controls in place, Byers says.

The most common scenario that would require a company to secure an SAS 70 audit from its service provider is when the company outsources application processing such as payroll. "If you outsource a transaction process like payroll, then you probably want an SAS 70 — because the control is at the service provider," Byers says.

But not every outsourcing arrangement necessitates an SAS 70. For example, a company that uses contract employees from an IT service provider to help manage its applications probably doesn't need an SAS 70 from the service provider because control over the systems remains internal.

Likewise, if a company uses an outsourcer for certain application development activities but retains control over application testing and change control, an SAS 70 might not be required. "If management is providing all the control, you don't need to have an audit of the service provider," Byers says.

Some arrangements are particularly cloudy about SAS 70 requirements. In a hosting arrangement, it's important to determine who has control over updates to an application, Byers says. Additionally, even if a company retains control over application testing and updates, an SAS 70 audit might be required to assess physical and environmental controls at the service provider's site, Byers says.

Even if an SAS 70 audit has been completed, it might not be adequate for SOX compliance, Meta Group says. The SAS 70 standard was developed long before SOX regulations and doesn't necessarily focus on the type of controls that SOX requires, according to the research firm.

There's no standard prescription for what is covered in an SAS 70 audit, Byers agrees. A service provider typically defines the control objectives and activities covered in an SAS 70 audit of its operations. "An SAS 70 can include as much or as little as a service provider wants. It's not a standardized audit report," Byers says.

Because the comprehensiveness of SAS 70 audits varies, it's up to the contracting company and its auditors to assess a service provider's SAS 70 for completeness and adequacy.

"Since the SAS 70 isn't standardized, you need to assess its completeness," Byers says. "Does it cover all your general computer controls? Does it cover applicable business process controls via the application controls?" In theory, a service provider could exclude areas from an SAS 70 audit where it knows it's vulnerable. But that's not typical, Byers says. In general, SAS 70 audits have become more comprehensive in light of SOX, he says. ■

MEANS A NETWORK THAT DOES MORE.

Procurve Networking by HP. More and more businesses get more from us.

MORE VALUE. Our solutions typically cost less. Much less.

MORE SECURITY. Our products can help detect would-be intruders at the edge of your network—before they reach the core.

MORE OPEN. We're interoperable. That means easy integration.

MORE INTELLIGENT. Run your network from the core. Control it to the edge.

MORE SUPPORT. Industry-leading support. Warranties that last a lifetime*.

MORE RELIABLE. Rigorously tested. Meticulously engineered.

MORE EXPERIENCE. We've been doing this for 25 years.

hp invent

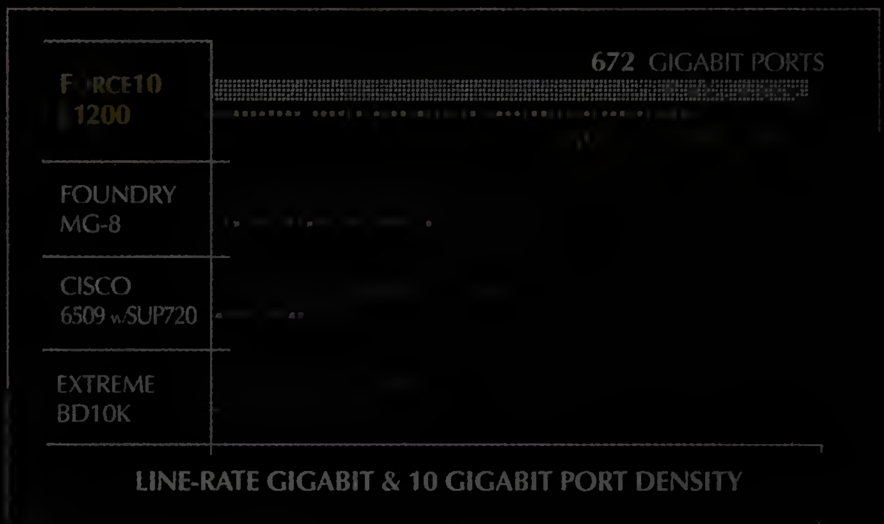
Find out more about ProCurve Networking. Call 800-975-7684 Ref Code 4 or download informative reports complete with case studies and cost-of-ownership analysis at **www.hp.com/network/moreprocurve.**

ProCurve Networking
HP Innovation

*Lifetime warranty applies to all ProCurve Products, excluding the ProCurve routing switch 9300m Series and Secure Access 700wl Series, which have a one-year warranty with extensions available. ©2005 Hewlett-Packard Development Company, L.P.

Were this a fine German car, you would ask for a test drive.

We offer this simple chart.



You admire precision engineering and seek out maximum performance. You want the best. Presenting the E-Series from Force10 Networks: The first resilient switch/router to deliver 672 line-rate Gigabit Ethernet or 56 line-rate 10 Gigabit Ethernet ports per chassis — more than twice the capacity of our competitors. That's Terabit performance.

Based on Force10's revolutionary TeraScale technology, the E-Series delivers industry-best metrics in density, throughput, resiliency and security. The advanced architecture of the E-Series ensures predictable performance with traffic-variation dampening, provides control plane resiliency to prevent DoS attacks, and supports line-rate, real-time security filters for high performance security.

To test drive the E-Series in your network, contact us at 1-866-600-5100 or visit www.force10networks.com.

FORCE10™

TOLLY 1st & Foremost CERTIFIED

To view independent TeraScale test results from The Tolly Group, visit www.force10networks.com

© 2004 Force10 Networks, Inc. All rights reserved. Force10, the Force10 logo, EtherScale, FTOS and TeraScale are trademarks of Force10 Networks, Inc. All other brand and product names …

Editorial supplement

NetworkWorld

March 21, 2005

The New Data Center

2nd in a six-part series

Piecing together the next-generation IT architecture

SPOTLIGHT ON SECURITY

- The next wave of security automation
- How to build a security operations center
- A look at security research projects

Plus: Visa takes on Web services with resolve and more

WHEN YOU STEPPED AWAY FROM YOUR DESK, A WORM WAS DETECTED, QUARANTINED AND ELIMINATED BEFORE ANYONE NOTICED YOU WERE GONE.

Cisco, Cisco Systems, the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the US and certain other countries. ©2004 Trend Micro Incorporated
All rights reserved. Trend Micro and the t-ball logo are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners.

Trend Micro and Cisco Systems— working together.

Imagine a network solution so advanced, so secure, so ingeniously proactive,
you may never have to worry about an outbreak again.

Find out more at www.trendmicro.com/cisco

Sam, don't lock them in. Get on Solaris™ 10!

What would you do with a 10,000 CPU grid?

Pay $1 to find out.

Introducing the *Sun Grid* for $1/cpu-hr. The network is your computer.

If you're paying more than $1/cpu-hr to build and run your own grid, you're overpaying. Because that's the price at which our grid is available to you. Pay $1/cpu-hr, and leverage our capital spend, SPARC® or x86 computers, storage, and facilities to run your business. From Monte Carlo simulations to reservoir simulation. Protein modeling to movie rendering. 1 cpu to as many as you could conceive. No minimum commitment, no maximum. Stretch your dollar at sun.com/sungrid

Sun microsystems
The Network is the Computer™

solaris Java

©2005 SUN MICROSYSTEMS, INC. ALL RIGHTS RESERVED. SUN, SUN MICROSYSTEMS, THE SUN LOGO, SOLARIS, THE SOLARIS LOGO, JAVA, THE JAVA LOGO, AND THE NETWORK IS THE COMPUTER ARE TRADEMARKS OR REGISTERED TRADEMARKS OF SUN MICROSYSTEMS, INC. IN THE UNITED STATES AND OTHER COUNTRIES. ALL SPARC TRADEMARKS ARE USED UNDER LICENSE AND ARE TRADEMARKS OR REGISTERED TRADEMARKS OF SPARC INTERNATIONAL, INC. IN THE UNITED STATES AND OTHER COUNTRIES.

The New Data Center

2nd in a six-part series

Piecing together the next-generation IT architecture

SECURITY AUTOMATION: THE NEXT WAVE

SECURITY COUNTERATTACK

HOW TO SOC IT TO THE BAD GUYS

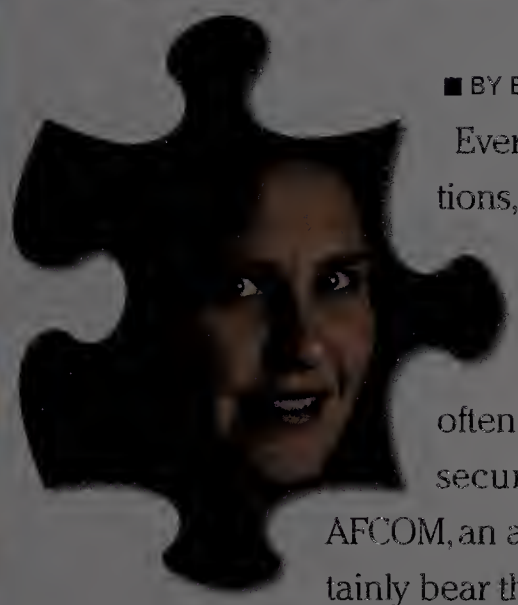
TAKING ON WEB SERVICES WITH RESOLVE

TECH TALK

WHEN TRUST ISN'T ENOUGH

From the editor

Security automation: A new data center mandate



■ BY BETH SCHULTZ

Everyone says they want to automate security functions, but few have done so fully. This is true even of the most mature security automation functions, such as intrusion detection, patch management and virus protection. Alerts are automated, but more often than not, responses aren't. The results of a recent security survey conducted for *Network World* by AFCOM, an association of enterprise data center managers, certainly bear this out.

In that survey, 99% of 157 total respondents identified the need to automate security functions as a "moderately important" or "critical" corporate strategic value (see related information, page 8). But only 14% of respondents said they automate responses for most types of alerts. The largest percentage — 44% of the respondents — reported handling all security alerts manually, with another 42% automating responses to only a few types of alerts. What's more, when it comes to managing security information, the largest percentage — 36% — rely on vendor point products rather than an integrated management platform.

However, progress is being made on the security integration front, as 28% report that they do integrate into a systems manager; 22% integrate into a security manager (14% indicated they do something other than run vendor point products or integrate into either a systems or security management platform).

Enterprise security won't ever be 100% automated — trust and cost are two factors prohibiting full automation. But security must become automated substantially enough as to become part of normal business operations.

Bringing that about means making security automation a core new data center component. Security functionality must be embedded in the network layer, for example, and companies must be willing to build security operations centers (SOC). Similar in concept to a network operations center, an enterprise SOC continuously monitors and manages a range of security devices and events to maintain and ensure overall network security.

This supplement explores these and other best practices for getting security to a more automated state. I hope we'll soon see less of a disconnect between the security automation ideal and today's reality.

— Beth Schultz
Editor, Signature Series
bschultz@nww.com

A look ahead to the other pieces of the 2005 New Data Center series:

Editor: Beth Schultz
Executive editor: Julie Bort
Designer: Brian Gaidry
Managing editor, fusion: Melissa Shaw
Online graphic designer: Eric Anderson
Copy editor: Ryan Francis
Network World editorial director: John G[illegible]
Network World editor in chief: John Dix

SPOTLIGHT ON SECURITY

Security automation: The next wave

Beyond virus protection and patch management

BY DEB RADCLIFF

Security automation. Isn't that the very nature of the beast? After all, just about any security process can be automated. Firewalls and intrusion detection systems and anti-virus software scan and sniff network traffic and computers for known signatures of attacks, viruses and worms. Vulnerability management systems find and patch holes, so malware can't exploit them. Remote access managers sandbox, scan and sanitize endpoints before allowing network access. And security managers get to view all of this and more from a central monitoring station.

OK, maybe it isn't an integrated monitoring station but rather a bunch of monitoring stations kludged into one console by a security administrator. That's the nature of the beast, too. The inability of different security products to share network and security information limits security automation. Limitations appear elsewhere, too. For example, intrusion-prevention systems (IPS) lack the intuition to know the difference between a

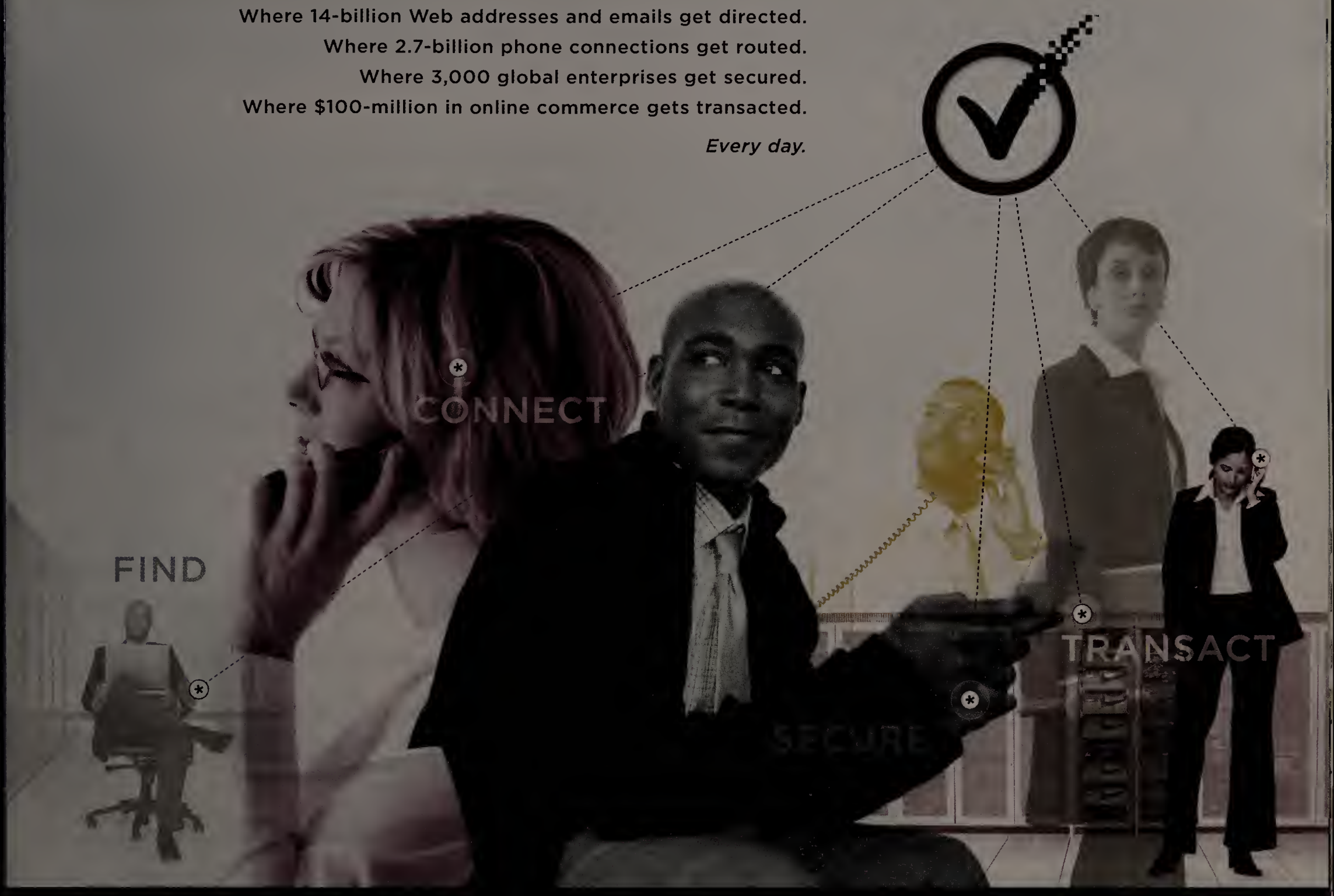
See Next, Page 38

Stand above the products, above the architecture, and look at the evolutionary process of where automation has happened.

—ROBERT CARIGUE, chief information security officer, Bank of Montreal Financial Group

Where 14-billion Web addresses and emails get directed.
Where 2.7-billion phone connections get routed.
Where 3,000 global enterprises get secured.
Where $100-million in online commerce gets transacted.

Every day.



VeriSign.®
Where it all comes together.™

Billions of times each day, the world interacts with a company you may not realize is there. One that is driving dynamic transformations at the very core of commerce and communications. VeriSign.® Through our Intelligent Infrastructure Services, we enable businesses and individuals to find, connect, secure, and transact across today's complex Internet, telecom, and converged networks.

We operate the systems that manage *.com* and *.net,* handling 14-billion Web addresses and emails every day. We run one of the largest telecom signaling networks in the world, enabling services such as cellular roaming, text messaging, caller ID, and multimedia messaging. We manage network and user security for over 3,000 global businesses and 400,000 Web sites. And we handle over 30 percent of all e-commerce transactions in North America, processing $100-million in daily sales. As next-generation networks emerge and converge, VeriSign will be there, deploying the Intelligent Infrastructure Services necessary for everything from RFID-enabled supply chains to inter-enterprise VoIP to mobile and rich media content distribution.

Whether you're a telecom carrier looking to rapidly deploy new services; a Fortune 500 enterprise needing comprehensive, proactive security services; or an e-commerce leader wanting to securely process payments and reduce fraud, we can help. We're VeriSign. Where it all comes together.™

© 2004 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, "Where it all comes together," and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries.

www.VeriSign.com
Download now: Free white paper on Intelligent Infrastructure Services

VeriSign®

Auto

continued from page S6

Christmas rush and a denial-of-service attack, which is why companies use intrusion prevention sparingly, or not at all. There's no way a security tool will ever be able to set policies aligned to your business' unique characteristics.

Suffice it to say, security will continue to become automated, but will never fully replace human perception, intuition and intervention. "You can build automated security models in a way to detect problems, establish countermeasures and alert a human, who can then build a filter or countermeasure to protect against that issue," summarizes John Pironti, enterprise architect and security consultant at Unisys. "In this way, there will always be a symbiotic relationship between humans and computers."

Know your business

Intrusion detection, anti-virus, firewalls and anti-spam are fairly mature when it comes to automation — meaning human intervention is minimized. While these tools needed manual updates and excessive filtering, they now essentially run themselves, by automatically updating their signature files, blocking worms and viruses, scanning and parsing datastreams, and looking deep into packets to detect bad behavior, says Vick Wheatman, vice president of security practices at Gartner. Reaching that level of maturation takes five to 10 years, analysts say.

They point to security information aggregation and identity management as two technologies at the other end of the maturation spectrum. This means we won't see mature automation of these disciplines until 2010 or beyond.

But don't just look to product trends to measure automation, says Robert Garigue, vice president and chief information security officer at Bank of Montreal Financial Group. Instead, organizations should focus on how security aligns with best practices and how it can be automated to the point that it moves from just security into the normal operations of the business, he says.

"Stand above the products, above the architecture, and look at the evolutionary process of where automation has happened," says Garigue, a frequent speaker on security maturation frameworks. "For example, firewalls are routine and so have become embedded in our network infrastructures. Patch updates and data quality have moved from exception management to normal operation."

When automated security becomes routine, security teams gain the freedom to deal with new risks and emerging policy issues. "Now we can focus on service-oriented architectures, digital rights management, identity management, and other emerging security issues that need best practices before they can be automated," he says.

In highly regulated industries, best practices and security automation go hand in hand. This is particularly true when it comes to proving who's accessed sensitive data and what events are happening on network segments where sensitive data resides, says Bernie Donnelly, vice president of quality assurance at the Philadelphia Stock Exchange.

"I was looking at security automation back in the '70s when I had to prove the same things three times to internal audit, external audit and [Securities and Exchange Commission] regulators," he says.

Over the years, as the Exchange diversified its trading system platforms, mainframe access controls no longer provided the audit trail regulators required. The new systems provided reams of report data that Exchange personnel needed to sift through just to get at the information in which regulators were interested, Donnelly says.

"We have all this log information, but from a security perspective, we're only interested in who's trying to get in and who's trying to go where they're not supposed to," he says.

So to prevent duplication of security and system expertise, the audit committee and security department created committees at the system and senior management levels. The committees then worked on ways to sort the data to find the exceptions to the company's audit and risk management policies, Donnelly says. Ultimately, the security team built filters to sift data coming from network and security logs. They installed Consul's InSight Security Manager to manage events and provide an audit trail of internal activity across the mainframe, Unix and messaging servers that make up the trading infrastructure.

"We wanted one system to bring this information together. So we worked with Consul because it's an offshoot of IBM [Remote Access Control Facility], which we still use in our environment. Consul gathers data from all three of our platforms into a central server, which we can query using a single language," Donnelly says.

Note that at the Exchange, as elsewhere, the process of narrowing the information down to manageable levels called for manually building filters. The human is still involved in querying the data to get to the important information.

"There are hundreds of potential information resources to draw security information from. The problem is narrowing it down from the 99% you don't care about to the 1% that you do," says Chris Byrnes, vice president of security practices at Meta.

The key to automating security event management is figuring out your sources and managing them down to a stream of information that is actually useful, then applying some automated correlation and analysis, he continues. Even correlation and analysis can't be fully automated because only the enterprise owners know what questions to ask the analysis engines.

"If you know what questions to ask these tools, they can provide you with answers. But you have to know what you're looking for and you have to specify the correlation rules. Right now, the vendors haven't done that in a way that's useable in multiple installations," Byrnes says.

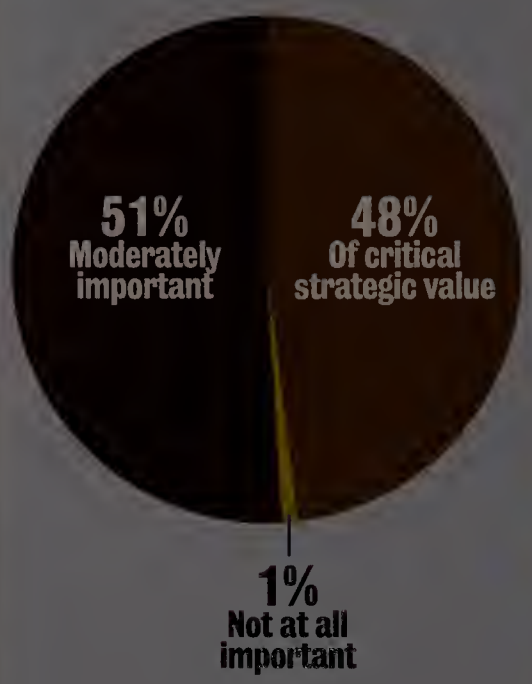
Furthermore, security information management (SIM) tools fail to take advantage of information already on the network — unless that information

See Auto, page S10

The automation imperative

Security automation has clearly become an IT mandate, with anti-virus protection, intrusion detection and prevention, and patch management the primary concerns, according to 157 IT professionals who participated in a membership survey conducted by AFCOM, an association of enterprise data center managers, on *Network World's* behalf.

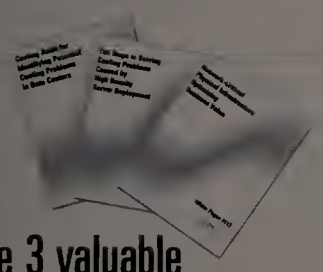
How important is security automation to your company's overall IT strategy?



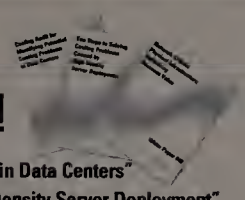
Which of the following technologies do you expect to be fully automated within your company within the next 18 months?

(Number of respondents)

More online! Head to Network World Fusion for results of the entire security automation survey. Use www.nwfusion.com, DocFinder:



Choose and receive any of these 3 valuable APC white papers within the next 90 days for FREE!



Choose and receive any of these 3 APC white papers within the next 90 days for FREE!

- ☐ White Paper #40 **"Cooling Audit for Identifying Potential Cooling Problems in Data Centers"**
- ☐ White Paper #42 **"Ten Steps to Solving Cooling Problems Caused by High Density Server Deployment"**
- ☐ White Paper #117 **"Network-Critical Physical Infrastructure: Optimizing Business Value"**

☐ **YES!** Please send me my FREE white papers. ☐ **NO,** I'm not interested at this time, but please add me to your mailing list.

Name: Title:

Company:

Address: Address 2:

City/Town: State: Zip: Country:

Phone: Fax: E-mail:

☐ ***Yes!*** ***Send me more information via e-mail and sign me up for APC PowerNews e-mail newsletter.*** **Key Code** w873y

What type of availability solution do you need?
☐ UPS: 0-16kVA (Single-phase) ☐ UPS: 10-80kVA (3-phase AC) ☐ UPS: 80+ kVA (3-phase AC) ☐ DC Power
☐ Network Enclosures and Racks ☐ Precision Air Conditioning ☐ Monitoring and Management
☐ Cables/Wires ☐ Mobile Protection ☐ Surge Protection ☐ UPS Upgrade ☐ Don't know
Purchase timeframe? ☐ < 1 Month ☐ 1-3 Months ☐ 3-12 Months ☐ 1 Yr. Plus ☐ Don't know
You are (check 1): ☐ Home/Home Office ☐ Business (<1000 employees) ☐ Large Corp. (>1000 employees)
☐ Gov't, Education, Public Org. ☐ APC Sellers & Partners

Key Code w873y

http://promo.apc.com

(888) 289-APCC x3314 • FAX: (401) 788-2792

APC®
Legendary Reliability®

©2005 APC. All trademarks are the property of their owners ISX4A4EB-USe • E-mail: esupport@apcc.com • 132 Fairgrounds Road, West Kingston, RI 02892 USA

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 36 WEST KINGSTON RI

POSTAGE WILL BE PAID BY ADDRESSEE

APC®

ATTENTION CRC: w873y
Department: B
132 FAIRGROUNDS ROAD
PO BOX 278
WEST KINGSTON RI 02892-9920

How to Contact APC

Call: (888) 289-APCC
use the extension on the reverse side

Fax: (401) 788-2792

Visit: *http://promo.apcc.com*
use the key code on the reverse side

APC®
Legendary Reliability®

Introducing data centers on demand

New architecture supports power densities of today... and tomorrow

Hot-aisle Ceiling Tiles/Cable Trough
Seals in hot air, prevents mixing with room air

WINNER 2004 BEST OF INTEROP NETWORLD|INTEROP

BLADE READY™

APC solutions that carry the "Blade-Ready" Logo are designed to handle the demanding network-critical physical infrastructure requirements of high-density blade server applications.

Chamber Doors
Access to hot aisle, locks for security

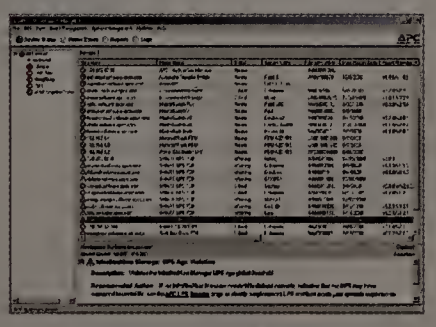
Now you can quickly deploy a standard- or high-density site of any size with scalable, top-tier availability.

Part Number	Usable IT Racks	Average kW per Rack	Price to buy	Price to lease (36 installments)
ISXCR1SY16K16P5	1	up to 5kW	$14,999*	$499**
ISXT240MD6R	6	up to 5kW	$149,999*	$4,999**
ISXT240MD11R	11	up to 5kW	$249,999*	$7,999**
ISXT280MD40R	40	up to 5kW	$699,999*	$21,999**
ISXT2800MD100R	100	up to 5kW	$1,649,999*	$50,999**
High Density Configuration *(shown above)*				
ISXT280HD8R	8	up to 10kW	$399,999*	$12,999**

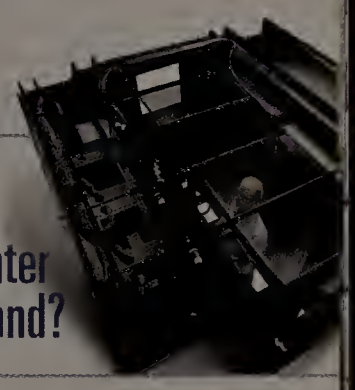
High density upgrades start at $10,999
On-site power generation options start at $29,999

All multi-rack configurations feature:

- ✓ *N+1 power and cooling*
- ✓ *Secure, self-contained environment*
- ✓ *Peak capacity of 20kW per rack*
- ✓ *Enhanced service package*
- ✓ *Integrated management software*



InfraStruXure™ Manager



What is data center on demand?

InfraStruXure™
DATA CENTERS ON DEMAND

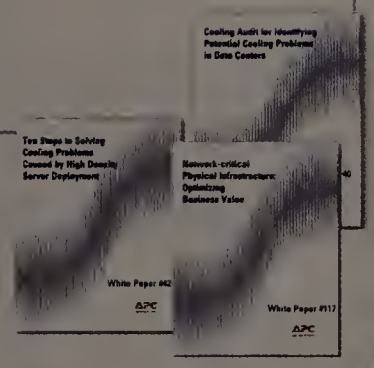
Highly available and manageable, quick-to-install, scalable architecture that easily supports both standard- and high-density applications.

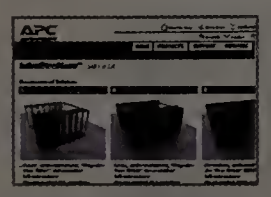
- *Up to 20kW a rack for any blade server application*
- *Unlimited racks*
- *Ships in 5 days****
- *Installs in 1 day****
- *Optional on-site power generation*
- *Raised floor not required*
- *Vendor neutral guaranteed compatibility*

Order your solution today. Call 888-289-APCC x3314.

Visit today and receive FREE APC White Papers

Visit us online and download APC White Papers.





InfraStruXure™ BuildOut Tool

Don't see the configuration you need?

Try APC's online InfraStruXure™ BuildOut Tool today and build your own solution.

Go to *http://promo.apc.com* and enter key code w873y Call 888-289-APCC x3314

APC®
Legendary Reliability®

* Prices do not include IT equipment and are subject to change. ** Indicative rates are subject to market conditions. *** Install and delivery times may vary.

©2005 American Power Conversion Corporation. All trademarks are the property of their owners. E-mail: esupport@apcc.com • 132 Fairgrounds Road, West Kingston, RI 02892 USA ISX4D4EF-USc

Auto

continued from page S8

comes from a product or system developed or supported by the SIM vendor. So gathering this information for deeper correlation and analysis usually means adding nodes and in-line devices all over the network.

"This is happening in both the wired and wireless spaces. It's the battle for the security management console," says Diana Kelley, executive security adviser for Computer Associates. "If we're going to automate, it has to be integrated and open. We have to be able to take information off IDS, firewalls and other reporting mechanisms in the enterprise, regardless of vendor. And for that, we need standards."

Look to standards

For the past two years, CA has been working with the IETF's Open Security Exchange to develop a common way of identifying and sharing security event information across multiple brands and types of devices. The Open Source Vulnerability Database, started at DEFCON in August 2002, to share common vulnerability definitions among vulnerability management systems is also available. And the IETF's venerable SNMP, which network management vendors have been using for decades, remains a must-have in the enterprise.

Coast Capital Savings is banking its security management future on SNMP. The Surrey, B.C., credit union, with 2,000 users in 50 retail operations, is rapidly expanding across Canada through mergers, acquisitions and new construction. To support the company's aggressive growth, Andrew Banman, senior system engineer, is developing a "branch in a box" template to get branches up and running with standardized security manageable at a single console.

"We need to come up with standards and boilerplate methodologies, tools and gear to support manageability that won't go out of date in a couple of years," Banman says. "The tools to do this are complex. The implementation is complex. So you need to step back and carefully plot a course."

Banman's team is working out an ambitious two-year plan to unify all security and management information using SNMP. Already, the team uses the FirePass SSL VPN box by F5 Networks to check the security integrity of remote machines against the company's security policy before allowing user access to the data center.

For its custom banking applications, the team is writing SNMP traps to track errors. And, from an infrastructure perspective, it's working with Cisco and 3Com to secure voice, video and data on the same stream.

"Monitoring all this data can become a huge nightmare. We'll buy where we can, write what we can, and use SNMP management to help unify it all," Banman says.

Leverage your infrastructure

Until all standards are as mature as SNMP, collecting and correlating security information from disparate devices continues to be an expensive and difficult undertaking.

Enter the attempts to integrate security management into switch management platforms: 3Com plans to integrate IPS technology acquired from TippingPoint Technologies early this year, Cisco last year introduced its self-defending network concept of secure access, IPS and security monitoring, and Enterasys Networks offers integrated anti-virus and policy management.

The University of North Carolina in Chapel Hill has embraced Enterasys' security management products to block viruses or attacks at the switch ports — a function the university gets without having to install a node on each of its 3,500 switches and 65,000 endpoints.

> **"Monitoring all this data can become a huge nightmare. We'll buy where we can, write what we can, and use SNMP management to help unify it all."**
>
> **— ANDREW BANMAN, senior system engineer, Coast Capital Savings**

When a hack or viral activity is detected on a specific port, Enterasys Netsight Atlas Console puts that computer into a remediation state until the computer is repaired, says Mike Hawkins, associate director of data networking at UNC. UNC uses Netsight Policy Manager to push traffic-blocking policies out to the edge switches in response to an ongoing threat.

Combined, the products significantly reduce the chance that malware might spread throughout the network, Hawkins says. "It takes less than a minute to stop an evil-doer. And with Netsight Policy Manager, we can respond in minutes to an ongoing threat," he says.

Determining where on the network — say the switches or routers — to take advantage of the vendor security management capabilities means setting objectives, Meta's Byrnes advises. "You need to ask yourself what data you most need to protect, what sources of information you'll need to do that protection and then start looking at what supports those sources," he says.

With the answers to these questions, you can align your security automation to the business, which is a far cry from automating everything, Unisys' Pironti says.

Understand user roles

As another example, take identity management. The capability to automate access management to every application on as fine-grained level as you can imagine exists, as long as you're not adverse to writing custom hooks for all your custom applications and any other applications with which the vendor product might not integrate. Yet from a business standpoint, automating user roles and provisioning resources is simply not feasible at too fine-grained a level, says Brad Bauch, a partner with PricewaterhouseCoopers' security and privacy practices.

However, those parts of identity management that can be easily automated already are moving out of security and into everyday operations — per Garigue's security-maturation model.

Bauch points to self-help password resets, which have clearly demonstrated ROI by reducing help desk calls by up to 70% in some organizations. And de-provisioning already is fully automated in his client sites and, for the most part, has become a human resources function. Furthermore, users can launch new account requests.

At Nextel, for example, employees and contractors can request their own user IDs via a Thor Technologies' identity management system that sits in front of the company's PeopleSoft HR application. A user ID request sets off a workflow e-mail for provisioned resources.

But Nextel says it doesn't provision fine-grained attributes for user roles and the resources unique to those attributes because of the time involved in developing such a system across hundreds of custom applications, says Tom Deffet, director of IT strategy and architecture at Nextel.

"The work it would take to automate provisioning of every combination of role and application boggles my mind," Deffet explains. "So we plucked the low-hanging fruit that we could get to quickly. It's not our ambition to get every piece of fruit off that tree."

Nextel set up four gross user roles — employee, contractor, business partner, customer — and automatically provisions access to resources common to all users within those roles. For example, resources allotted to the employee include LAN, e-mail, VPN and Internet access. In another year or so, Nextel says it hopes to develop more detailed attributes, such as department and job title.

For the second phase, which entails business partner self-registration, Nextel had to wait for its Web access control vendor, Netegrity, to adopt the Organization for the Advancement of Structured Information Standards' Security Assertion Markup Language (SAML). Nextel wanted SAML to support delegated administration, he says.

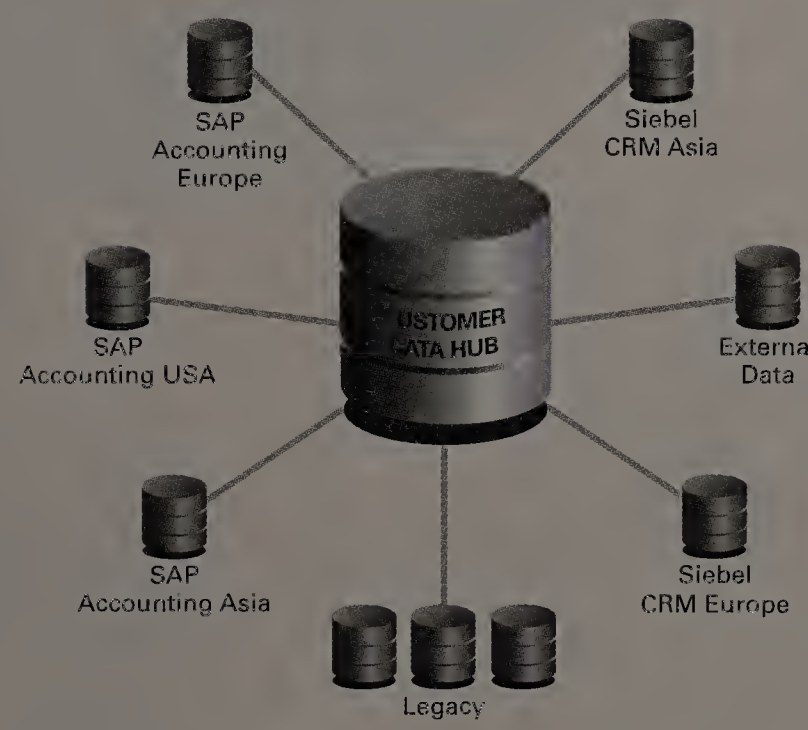
That phase rolled out late last year. Now Deffet's team is looking into ways it can use federated identity standards to give Nextel employees access to applications outsourced to its business partners.

Such is the pattern with all security automation, Garigue says. First you identify the risk, then develop standards and finally, you automate best practices. This pattern will repeat itself far into the future, particularly as companies deploy new data center architectures for distributed and service-oriented computing, he adds.

Radcliff (www.deb.radcliff.com) is a freelance writer specializing in online safety and network security.

Oracle Customer Data Hub

All Your Customer Data In One Place



All your applications can share consistent customer data in real time.

ORACLE®

oracle.com/datahub
or call 1.800.633.0940

Copyright © 2005, Oracle. All rights reserved. Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Security counter attack

SPOTLIGHT ON SECURITY

Four experts share the latest research-and-development news.

■ BY SANDRA GITTLEN

If you think re-architecting your IT infrastructure with new data center technologies will help protect your company over the next decade — think again. Experts at academic and vendor research labs around the country agree the move toward an automated, on-demand, virtualized computing environment will increase the complexity of security.

With the new data center, IT executives "won't be able to think of the enterprise as a castle with a drawbridge and one point of entry to keep the bad guys out. They'll have to look at every node in their network, every computer in the network, as something to defend individually," says Dirk Balfanz, a researcher at the Palo Alto Research Center (PARC) in California.

PARC is just one of many organizations focused on solving security problems that lie ahead. Among researchers' goals are reining in complexity, improving identity management and developing platforms to protect digital assets.

"Complexity is the enemy of security," says Ed Skoudlis, an instructor at the SANS Institute in New York. "The constant drive for new innovation and new functionality introduces complexity. And this complexity introduces flaws."

Wireless networks, Web services and other emerging architectures will pose challenges for IT managers, Skoudlis says. "They'll need to apply security at different layers in the network. You have security layers for the older technology, and then you'll need more for the new architectures," he says.

Researchers at PARC concur, and so they have been researching ways to prevent users, confronted with security mechanisms at too many layers, from ignoring or, worse, tampering with security procedures. "If a security procedure is too difficult, users won't deploy it. They may configure it incorrectly, or they'll just switch it off," Balfanz says, citing a PARC study that found enabling laptops with 802.1X security took users two hours. Rather than struggle, users stopped using the security features of the network which jeopardized network data, he says.

PARC's Security Research Group developed an architecture that eliminates these frustrations for users while letting IT organizations employ tighter security. With this architecture, users connect their laptop to an "enrollment station" via a close-proximity technology such as infrared. After being authenticated by the enrollment station, the user gains network access and then receives a digital certificate that automatically configures network policy settings on the laptop. The whole process takes less than 2 minutes, Balfanz says.

PARC is working with vendors to put this architecture in enterprise products.

Language-based security

Programming techniques, including those used in creating Web services, are the focus of security researchers at Cornell University in Ithaca, N.Y. "Web services are being built with vulnerabilities" that could spread rapidly as Web services are shared across networks, says Fred Schneider, director of the Information Assurance Institute at Cornell. "If you're building off of something else, you might not understand the properties of everything you're working with. Security is not something you can evaluate by looking at the interface," he adds.

RICCARDO STAMPATORI

His research team, in cooperation with Intel and the Office of Naval Research, is working on a project called Language-Based Security. The aim is to put basic tenets of solid security, such as in-line reference monitors, information flow policies, proof-carrying code and certifying compilers, into emerging technologies.

Schneider also advocates the use of safe systems languages that work much like the common C language. The hope is that bringing these practical components into newer applications such as Web services will shore up flaws that extensible systems could generate, he says.

Security and privacy

Ken Klingenstein, director at the Internet2 Middleware and Security Initiative, says he's not optimistic about the ability for complexity to be reduced. "Short-

See Labs, page S14

EMC²
where information lives®

Fr: expecting the world from Oracle

To: getting the universe

EMC CAN HELP YOU OPTIMIZE ORACLE ACROSS ITS ENTIRE LIFECYCLE. Our services, software, and hardware help you get more from your Oracle database and applications. Developed jointly with Oracle, our solutions give you the power to improve availability, reliability, and flexibility while lowering TCO. You gain a common information infrastructure, proven to work in the most demanding situations — including migrations, upgrades, backups, and peak workloads. Visit www.EMC.com/solutions to learn more and sign up for a live demo. Or call 1-866-464-7381.

Find an authorized EMC Velocity² Partner at www.EMC.com/velocity.

EMC², EMC, and where information lives are registered trademarks of EMC Corporation. © 2004 EMC Corporation. All rights reserved.

Labs

continued from page S12

sighted solutions, deep vulnerabilities and the nature of how complexity compounds over time means we're in for difficult times," he says.

But improvements are possible in the way resources are shared across the Web, while user privacy is protected, Klingenstein says. "What seemed to be orthogonal goals of security and privacy can be achieved together," he says.

The Internet2 created the Shibboleth Project to address the need for simple, secure cross-organizational data access. The Shibboleth System, which comprises open source identity provider and service provider components, lets network users access resources inside and outside their organizations without suffering through multiple registration processes. They do not need to offer personal information unnecessarily.

"The goal is to have users release only the minimum amount of information to content providers to determine whether they are eligible for that content," Klingenstein says. This will help reduce identity theft and fraud, he adds.

Using common security standards such as the Security Assertion Markup Language from the Organization for the Advancement of Structured Information Standards (OASIS), public-key infrastructure and X.509, the Shibboleth System requires a content provider to employ the service provider software and a user to be part of a network that uses the identity provider software. Say an academic goes to another university's resource site that is running the Shibboleth service provider component. He will be required to select among organizations that have site privileges. Once he chooses his university, the browser automatically will send him to his university's sign-on page, which runs the identity provider software. The academic then logs on, as he normally would with the familiar name and password and when he is authenticated, he is sent back to the destination resource site and is free to access information there.

Shibboleth already is being put through its paces within the enterprise. The Pennsylvania State University has tested the system to allow students secure access to the college's Napster music service. Meanwhile, the grid computing community has embraced Shibboleth as a key security technology.

On the flip side, content providers are panicked that the distributed nature of data centers — with detached devices and on-the-fly extended enterprise partnerships — lessens their control and jeopardizes the security and integrity of data. In an era of compliance and regulatory restrictions, this is unacceptable.

But content management researchers are working on digital rights management platforms that would solve this problem — securing data even if it is out of the network's reach. IT organizations "need to understand where and how data is being used," says Hari Reddy, director of business development at ContentGuard, founded by former PARC researchers. "How can you manage data when it leaves your security framework?" He points to extended enterprises and the sharing of data as one complication. "I may want to stop the specific usage of data [we've exchanged] at some point."

Companies must be able to map policies to data and have those policies act as authorization tools, he says. "People not only want to manage how data is consumed, but also how it is distributed," he says.

ContentGuard continues to develop eXtensible Rights Markup Language (XrML), a de facto industry standard submitted to OASIS and other standards groups as the basis for any digital rights language specification. XrML extends the range of rights-enabled business models for digital content and Web services. It lets IT managers place detailed restrictions on content that is distributed beyond the enterprise walls and lets them manage the life cycle of data and Web services.

For example, a company might place a control to distinguish those who are allowed to use the data or Web service vs. those who can distribute it. "This allows the creator of the data to say, 'Alice has the right to view it, but Boston University has the right to license and distribute it,'" Reddy says.

XrML is part of a multitiered distribution architecture that must feature a time element to limit how long data is valid, Reddy says. A CFO could set an expiration date of 30 days past publication when distributing financials or a vendor sending out a technical manual could mark the material as invalid after six months. This context and control is needed as data gets further from its origin.

He says the content store, which used to manage data inside the network, would become the manager for data no matter where it flows.

Gittlen is a freelance technology editor in Northboro, Mass. She can be reached at sgittlen@charter.net.

The biggest security challenges ahead

Six researchers answer the question, "What are the most critical security issues facing IT?"

"A big challenge for IT managers will be cross-site scripting attacks. Hackers are able to corrupt SQL queries in Web forms and preempt what an application is intended to do. We don't have tools to stop that and it requires an understanding of what the interface needs to do to block the attack."

— **Fred Schneider,** director of the Information Assurance Institute at Cornell University, Ithaca, N.Y.

"Radio frequency ID tags are going to be very easily hacked. That has serious implications because use of these tags is being proposed in a lot of applications . . . . RFID technology should not be moved into high-security applications without attention to authentication protocols and repudiation methods."

— **Mich Kabay,** associate professor for information assurance at Norwich University, Northfield, Vt. (see www.nwfusion.com, DocFinder: 6323)

"The trustworthiness of an automated system is tied to the integrity and quality of the information that is shared between systems. This requires new trust models and identity constructs. In some instances, messages will be sent by entities that are unable to provide strong credentials in the form of digital certificates. Automated systems will need to be able to infer trust based on other types of indicators."

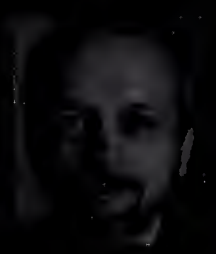
— **Bob Gleichauf,** CTO, Cisco's Security Technology Group

"Spam on wireless devices is going to be a significant challenge. CIOs are paying to download every megabyte of data across multiple channels. They don't want to bear that cost. These devices are just not secure enough for the mass market yet."

— **Dave Steer,** director of segment marketing, ARM

"The privacy issue is going to be more complicated because Big Brother can know who is doing what, where, how and when. Integration of biometrics in security is going to be much tighter. . . . And there are going to be more devices to secure and more systems that are going to require different types of access and control. I'd like to think that there's going to be distributed systems where you can write policies to provide controls to these devices."

— **Sharon Besser,** director of security solutions, Check Point



"The problem is that a majority of enterprise data is no longer on servers — it's on the clients. The bad point of this is that a lot of security threats emanate from clients. I'd worry less about the man-in-the-middle sniffing and more about the endpoints and people walking off with laptops."

— **Charles Palmer,** department manager for security, networking and privacy, IBM Research

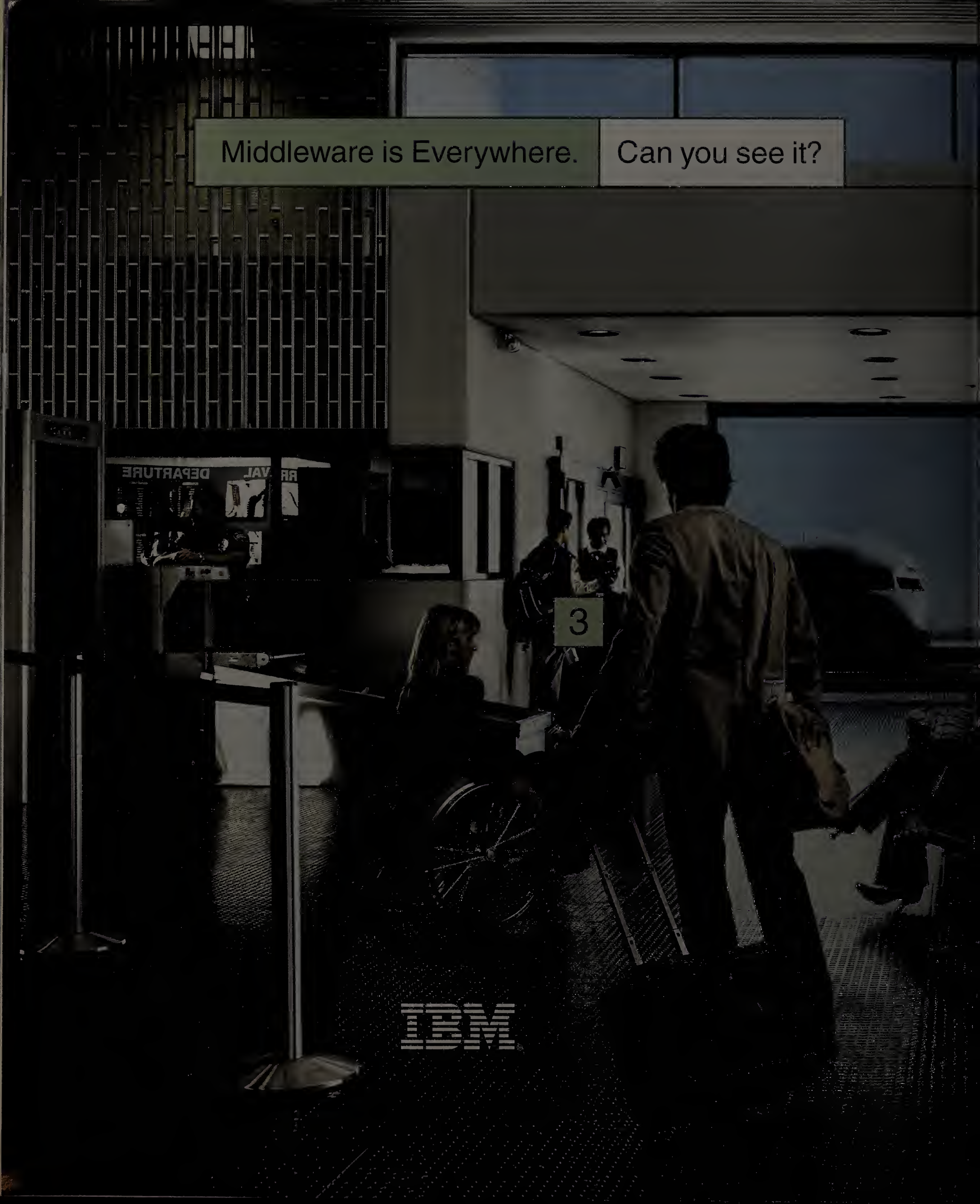
Tivoli | **Key**

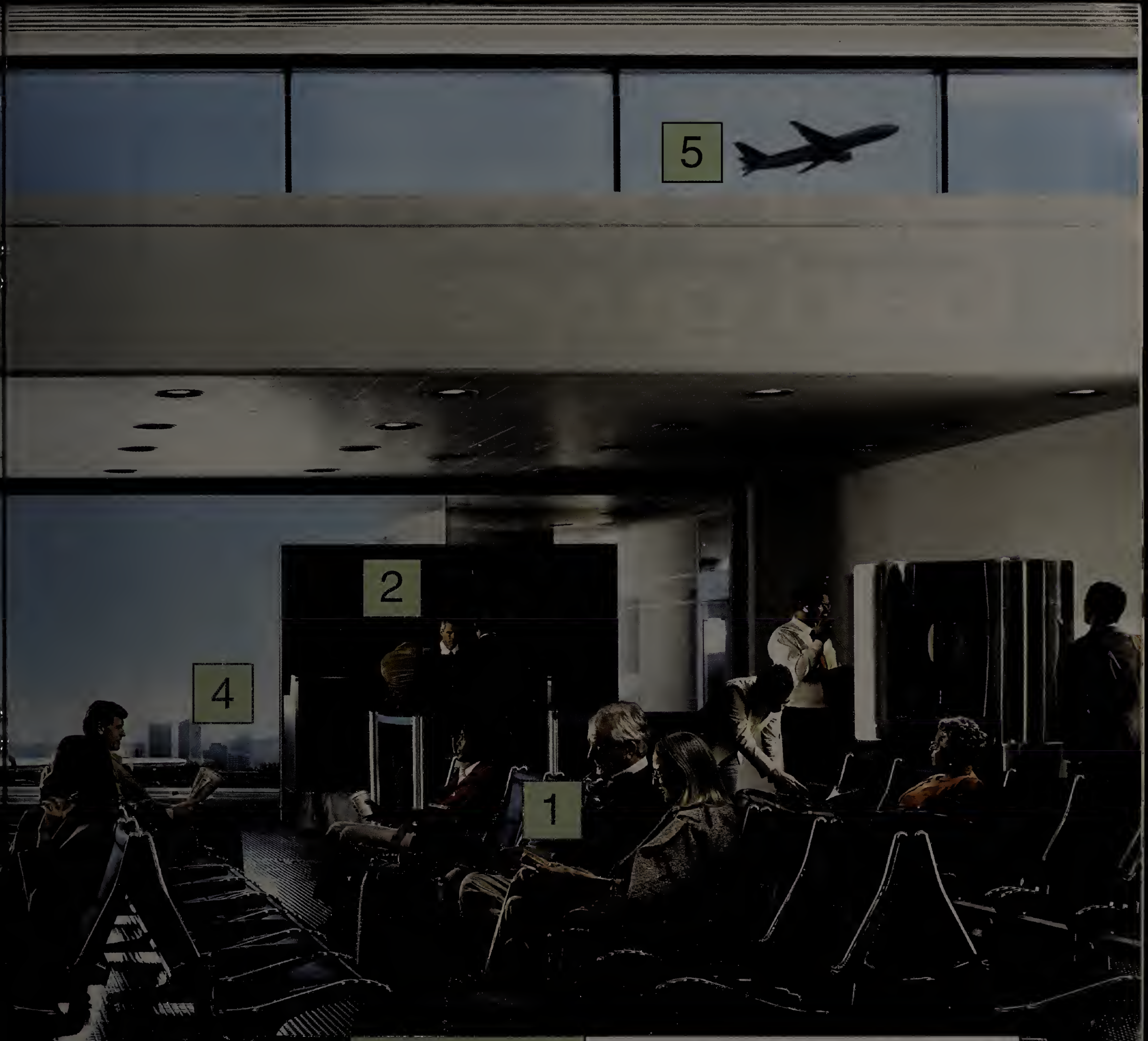
1. **Buyer downloads competitive pricing.**
2. **Manager securely retrieves invoices.**
3. **Driver obtains specific delivery details.**
4. **Ex-vendor denied access to intranet.**
5. **Customer's identity protected from theft.**

MIDDLEWARE IS IBM SOFTWARE. Identity management software that uses single sign-on technology to ensure that the right access is given to the right people. Open, modular Tivoli security software that automates processes between employees, partners, customers and suppliers – while helping to reduce costs. It's how everyone involved gets the information they need. On time. And on demand.

Middleware for the on demand world. Learn more at **ibm.com**/middleware/identity ON DEMAND BUSINESS™

IBM, the IBM logo, Tivoli and the On Demand logo are registered trademarks or trademarks of International Business Machines Corporation in the United States and/or other countries. © 2004 IBM Corporation. All rights reserved.


Middleware is Everywhere.
Can you see it?
DEPARTURE
3
IBM



DB2.

Key

1. **Takes virtual tour of vacation spot.**
2. **Books flight with partner airline.**
3. **Dispatches service automatically.**
4. **Analyzes schedule data dynamically.**
5. **Business results reach new heights.**

MIDDLEWARE IS IBM SOFTWARE. The powerful DB2 Information Management Software Family. With industry leading DB2 and informix® databases, it's the most complete information management solution available. Built on open standards, it lets you access content from various sources. Integrate information, boost productivity, stay compliant. Plus gain insight to make better business decisions. On demand.

Middleware for the on demand world. Learn more at **ibm.com**/information ON DEMAND BUSINESS™

IBM the IBM logo, DB2, Informix and the On Demand logo are registered trademarks or trademarks of International Business Machines Corporation in the United States and/or other countries. © 2005 IBM Corporation. All rights reserved.

How to SOC it to the bad guys

A security operations center is becoming an enterprise must-have.

SPOTLIGHT ON SECURITY

■ BY JOANNE CUMMINGS

Eamus Halpin's wake-up call was the Slammer worm. Until it hit, he had relied solely on port blocking to protect his enterprise network from hacks and intrusions. After he saw the network carnage Slammer wreaked around the globe, Halpin knew he had to revamp his company's approach to network security.

"I happened to be with Microsoft at the time at an NDA event in Seattle, and somebody scared me about what could happen to a port blocking-based network hit by Slammer," recalls Halpin, who is chief technical architect at iRevolution, a managed services provider in London. Although iRevolution's network was spared a direct hit by the worm, Halpin knew that had just been luck. "I spent three hours researching the implications of the worm, and my hair went white. We were as open as Swiss cheese," he says.

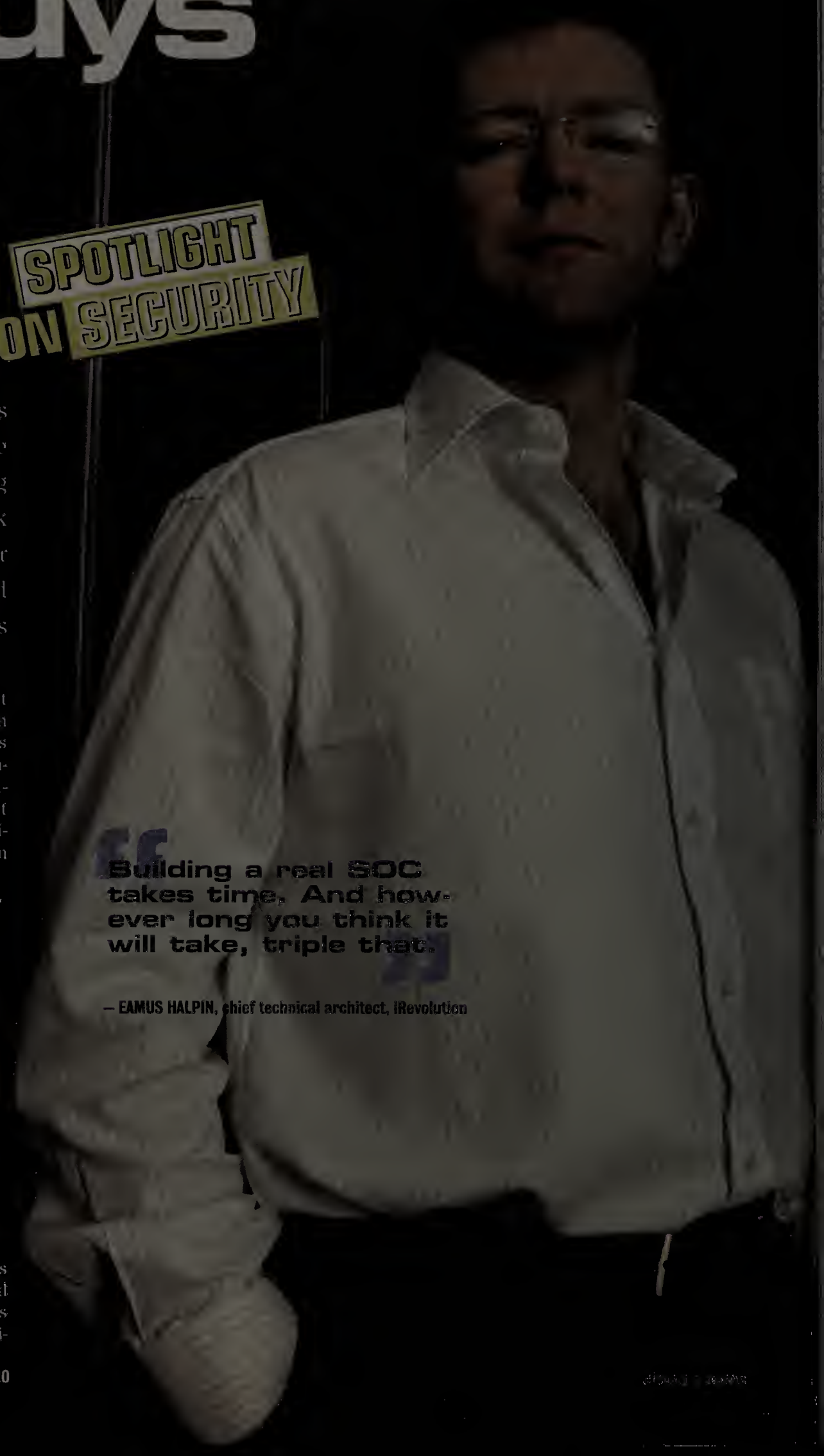
Although iRevolution had the basics in place — firewalls, anti-virus software, intrusion-detection systems (IDS) — it had no way to combine alerts from these various security tools to build a logical picture of the security health of the network.

"Everything was separately maintained and managed. They didn't speak to each other and didn't give us a business temperature for the enterprise as a whole," Halpin says. "So we could see occasionally that we were being attacked by a particular type of virus through e-mail, but we couldn't really determine how big an issue that was in the great scheme of things."

Halpin decided then and there to do a complete security overhaul. His goal was to build and maintain a world-class security operations center (SOC) for iRevolution's internal network, as well as to help support customers.

Just as network operations centers (NOC) continuously monitor networks to mitigate faults and ensure optimal performance, SOCs continuously monitor and manage a range of security devices and events to maintain and ensure overall network security. Experts say SOCs are becoming more common among companies for a variety of reasons, most notably

See SOC, page S20



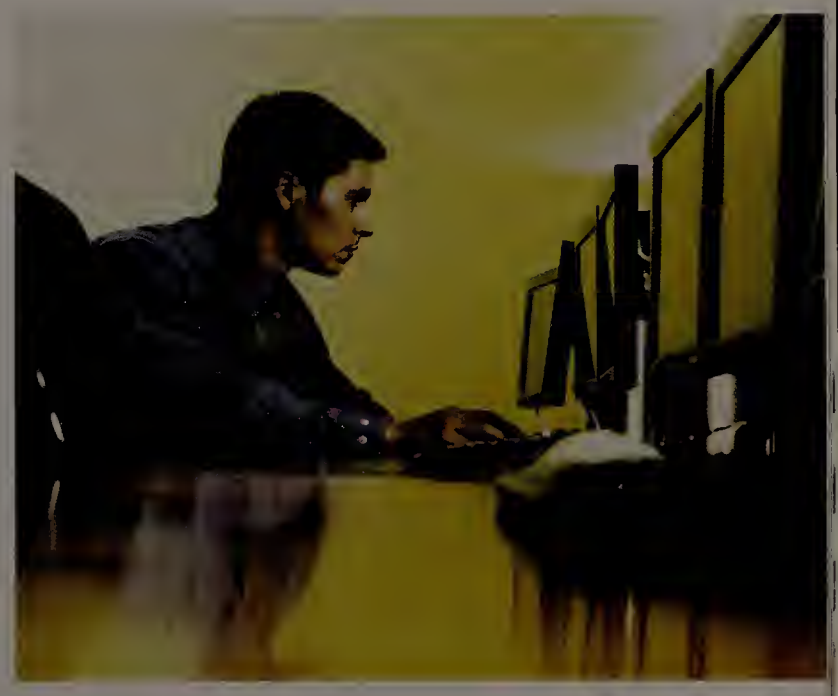
"Building a real SOC takes time. And however long you think it will take, triple that."

— EAMUS HALPIN, chief technical architect, iRevolution

Application Performance

Solving Application Performance Problems

A Proactive Approach



Poor application performance is a problem with which many IT departments are all too familiar. An August 2003 study by Network World and Packeteer found that more than 60% of the IT respondents had experienced significant application performance degradation – a number that climbed to nearly 85% for companies with revenues exceeding $1 billion.

This problem has negative effects throughout a business, from reduced employee productivity to increased customer dissatisfaction and loss of business. It also significantly reduces IT department efficiency, as staff members are repeatedly pulled away from development projects to troubleshoot performance issues.

Why monitor application performance?

Companies have many reasons for monitoring application performance.

A major insurance company wanted to proactively track compliance with service level agreements (SLAs). The company also wanted to test how infrastructure changes (such as consolidating servers) would affect end-user response times, as well as reducing troubleshooting time by seeing exactly what was happening at the time a problem occurred.

A large financial services company considers good application performance to be an end in itself. "Efficient operation of our networked applications is a key element in attaining our corporate vision," says the company's IT manager. "In addition to delivering high levels of performance to our large user base, we need to make sure that new applications won't introduce performance bottlenecks before rolling them out."

A major northeastern commercial bank values good application performance because it maintains end users' productivity – so when problems do occur, the bank needs to troubleshoot them efficiently. "We were spending a minimum of 20 hours a month – sometimes up to two or three weeks – trying to diagnose the cause of application slowdowns," says a network engineer. "We just didn't have the staff to keep doing that." A particular problem, he notes, was trying to determine if a slowdown was a network issue or a server issue. "When our network team thought it was a server problem, the server team would often claim it was a network problem," he said. "It was difficult to pinpoint the exact trouble spot."

Fluke Networks SuperAgent to the rescue

All three of these companies have found that Fluke Networks' SuperAgent Application Performance Analyzer provides accurate, detailed insight into end-user response times throughout the enterprise. As a result, IT staff can quickly determine whether a problem is network, application, or server related and can rapidly resolve the issue.

> **"When our network team thought it was a server problem, the server team would often claim it was a network problem. It was difficult to pinpoint the exact trouble spot."**
> – Network engineer from a major commercial bank

For example, according to the insurance company's IT manager, "SuperAgent helps us better serve our end users by being proactive with application performance issues – and being able to more effectively baseline application performance helps us ensure that we meet our established Service Level Agreements for transaction times." When problems do arise, he notes that SuperAgent "can mean the difference between a one-hour slowdown and a one-day slowdown."

The financial services company has found that SuperAgent helps with everything from service level management to resolving performance issues to capacity planning. The solution also has virtually eliminated finger pointing and wasted cycles. "Before, we could easily spend four hours trying to determine the cause of the problem," says the director of network operations. "With SuperAgent monitoring the network core, we can identify the trouble cause in about 15 minutes." As a result, development teams spend their time creating and deploying needed applications rather than being bogged down resolving problems.

The commercial bank finds that SuperAgent's performance monitoring capabilities make the IT department more proactive, identifying and resolving problems before users are even aware of them. The tool's enhanced troubleshooting capabilities save them at least 20 hours a month – plus it has made a big difference in the relationship between the network and server teams, replacing finger pointing with cooperation. "Now the server team comes to us when they have a problem and asks us to monitor their servers," says a network engineer. "We also get requests for troubleshooting help from other business groups in the main office. They all think SuperAgent is fantastic – they are overwhelmingly impressed with its reports." He also describes a case where slow performance of a vendor-hosted application was causing a department to fall behind in its work. SuperAgent identified the vendor's server as the source of the problem, and the vendor – who hadn't previously been aware of the difficulty – was able to quickly fix it.

The bank is so impressed with SuperAgent that it soon will be performing full server monitoring, with reports on server availability and alerts when utilization levels exceed a fixed percentage. It will also use SuperAgent's results to set up SLAs with its branch offices, so it can demonstrate compliance with agreed-upon availability and uptime figures. "We just couldn't do any of this without SuperAgent," concludes the bank's network engineer.

For more information about application performance management solutions visit ***www.flukenetworks.com/APM***

FLUKE networks

©2005 Fluke Corporation. All rights reserved

SOC

continued from page S18

discipline based on point solutions to something far more pervasive and critical to overall network health.

"It used to make sense to have security specialists managing the various firewalls, IDS and so on because security was at a very specific location on your network and had a very specific function," explains Andreas Antonopoulos, senior vice president and founding partner at Nemertes Research. "But security no longer works that way. The perimeter is porous, and instead, security needs to be applied at the application level, at the network level and at the storage level. It's become a feature of your end-to-end application delivery, much like network performance."

— ANDREAS ANTONOPOULOS, senior vice president, Nemertes Research

Regulatory pressure brought on by the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act and the Gramm-Leach-Bliley Act also drives enterprise SOC development.

"SOX is a good example of a proactive driver for SOCs," says Diana Kelley, executive security adviser at Computer Associates' eTrust division. "You've got to be ready for 404," she says, referring to the section of SOX that explains that executive management needs to take responsibility for establishing and maintaining an adequate internal control structure. "That means you need the correct and effective controls on your business reporting. And once you have them, you need to monitor and maintain them, and a SOC is an effective way to do that."

According to preliminary research by Nemertes, the average U.S. organization plans this year to up its security budget 100%, from 2.4% of the IT budget to 4.8% — an increase Antonopoulos attributes almost entirely to regulatory compliance. "I can tell you that all those companies that are doubling their budget to do regulatory compliance are looking at either building a SOC or re-engineering a SOC to comply with the regulations," he says.

The trend to pull back security monitoring duties previously outsourced to managed security services providers (MSSP), especially in the financial services sector, adds fuel to the fire. An internal SOC allows better control and visibility into the enterprise network, and reduced costs overall, says Jim Tiller, chief security officer and vice president of security services at International Network Services, a network consulting firm.

"MSSPs are having difficulty responding in some cases," Tiller says. "With the regular occurrence of worms and denial-of-service attacks, especially in the financial industry, and the increase in our vulnerability and the sophistication of those threats, the ability to respond is strictly related to how much visibility you have in your network. By pulling the management in, you have more visibility and can facilitate the ability to respond."

Plus, "for large companies, the investment in managed security services is fairly significant and they're seeing long-term cost/benefit with regard to pulling that in-house and managing it themselves," he says.

The hurdles

Although recognizing the need for a SOC is fairly easy, building one is not so straightforward. This is especially true when the security and network operations groups have grown up independently. Security monitoring might be robust, but if it is separate from network operations monitoring that can be a recipe for disaster, experts say.

"Security events don't always appear as security events," Antonopoulos says. For example, if a router stops responding and that's all the information you have, it's difficult to tell if it's a network problem, a systems problem or a security problem. If your network operations group is completely separate from your security operations group, one of two things will happen: "Either both groups will chase the problem separately, or worse, neither will chase it, concluding that it's the other group's problem," he says.

This confusion is exacerbated when it comes time for remediation. "If both organizations are implementing things on the network and monitoring it, you may come to the point where the network people are changing [access control lists], reducing your security, or your security people are applying ACLs that are impacting network performance," he says. "Since you're not integrating this and looking at it from an end-to-end perspective, you end up with problems."

A true SOC integrates security and network event information so the security and operations staffs have an overall view of the event and the effect it's having on the network, and can make informed decisions about how best to react according to predefined security policies. But that's easier said than done.

See SOC, page S22

Five SOC pitfalls to avoid

1. Technology tunnel vision. Getting caught up in the latest and greatest tools is tempting, but the core of your security operations center (SOC) should be based on sound risk assessment and security policies. Once you've hammered those out, you can focus on the products and technologies that will best support them.

2. Silo mentality. Don't organize your SOC in a silo separate from your network operations. An efficient SOC depends on fully integrating security and network monitoring tools, as well as the staffing associated with them.

3. Staffing mistakes. Don't use your veteran security staff to do low-level monitoring, and make sure you have the proper checks and balances in place so that no one person holds all the keys to your network kingdom.

4. Inflexible tool sets. Choose tools that will support not only your current security devices, ticketing systems and network monitoring suites, but also those that are easy to customize and offer a variety of templates and wizards. Be aware that even the best tool sets require a good deal of customization and integration.

5. Taking the cheap route. A SOC is no place to skimp. On average, large organizations should plan to invest $1 million or more to implement and maintain a truly enterprise-level SOC. And that investment will most likely grow over time.

— Joanne Cummings

©2004 DuPont or its affiliates. The DuPont Oval, DuPont™ and The miracles of science™ are registered trademarks or trademarks of DuPont or its affiliates.

YOUR COMPANY'S FIREWALL

Introducing DuPont™ certified limited combustible cable. In the event of a fire, securing your business' uptime is crucial. The data communications cable you choose could play a key role in protecting your network technology investment. DuPont™ certified cable produces 20 times less smoke than other plenum rated cables. And less smoke means less costly downtime, making it the most advanced fire safety cable technology available today. *To learn more about DuPont™ certified limited combustible cable or to request a free CD, log on to teflon.com/cablingmaterials or call 1-800-207-0756.*

DUPONT

The miracles of science™

SOC

continued from page S20

Where to start

Many organizations first look to purchase a security event management system or alert correlation engine. But experts say that's a tactical mistake. An overall risk assessment, for determining the actual business importance of each network asset, must come first in the SOC project.

"You have to apply your resources to protect the things that are most important to you," says John Summers, global director of managed security services at Unisys. "Some IT execs have a very good handle on their infrastructures. They know what assets are out there and what's running at each IP address, but very few can tag a business priority to their infrastructure elements."

Knowing the business importance is key because the purpose of a SOC is to enable not only security event monitoring but also confident responses to those events. "So if this server went down, what would it mean to the business, and is this server more important than this other one? Once you know that, the technology part tends to fall into place," says Summers, who manages Unisys' three major SOCs.

Technology caveats

Choosing a technology platform comes next. The goal is to find a security event management platform that can work with the variety of security devices you have in place, correlate their various alerts, and provide some form of integration with whatever you are using for trouble ticketing and network operations management. Organizations need this depth of visibility into the network to ferret out security breaches, experts say.

"A big financial services company we work with was seeing some poking at different areas of its network around the globe," CA's Kelley says. "Each of the pokes didn't look particularly bad individually, but they were all coming from the same IP address over a period of a couple of days. None of it was enough to trigger an alert on its own, but once the company pulled that information into a centralized console [within its SOC] and saw what this one IP address was doing to its network around the globe, things started to add up."

However, getting to the point where you can have such a global view within your SOC is time-consuming and expensive.

In addition to integrated security event managers from start-ups such as ArcSight, Intellitactics and netForensics, most of the large network management companies — CA, HP and IBM — offer a security event monitoring capability integrated within their platforms. But they all come at a pretty hefty cost.

"In the security space, IDSs generally don't speak the same language to your management system that your firewall does," Nemertes' Antonopoulos says. "If you want to add a rule into your firewall to block something, you can't use the same language you would use to add a rule in a router. As a result, security event monitors require a large integration project to pull all that information, turn it into a common format and correlate it across all those domains."

The vendors pass on the cost of that large integration project to their customers. The hardware and software for these packages alone costs on average $1.5 million to $3 million, Antonopoulos says. "Add to that three shifts of people and the integration into a ticketing system, and it gets very expensive," he says.

IRevolution's Halpin says his SOC project, which is based on CA's Unicenter for network management integrated with CA's eTrust for security monitoring and event correlation, costs approximately $1 million and took 18 months to implement. The SOC has been up and running for about six months, and Halpin says he's just now feeling like he's getting worthwhile and actionable information from it.

He negotiated a "fair" contract with CA, "but the majority of my costs are in people time," he says. That's because picking the tool is one thing but getting it tuned to your particular environment takes time and troubleshooting.

"Anybody who's up for this and wants to see a pretty center with blinking lights can get that in 10 minutes," Halpin says. "But building a real SOC takes time. And however long you think it will take, triple that, and then be prepared to maintain it. This isn't easy and it's never-ending."

He says one key to easing the process is to make sure the tool you choose is flexible. That means making sure that not only will it support the various firewalls, IDSs and network management platforms you have in place, but also is easy to customize and tune.

"It has to be easy to write rules," he says. "If you can write those rules quickly, and you have templates and good wizards for it, then that's going to make the whole process much easier."

But perhaps the biggest caveat for building a SOC is to realize that your initial million-dollar investment is just the beginning. Because technology is changing all the time, so will your security needs and strategies.

"Although I feel like our security and our SOC are very scalable now, I'm expecting that within three or four years' time, we'll have to throw the whole thing out and do something different because security will have moved on," Halpin says. "With the amount of processing power that is about to become available through dual-core and all of the other technologies, you can't stand still. Those things will have a significant effect on the technology and security marketplace, and we know here that security will always be an ongoing expenditure."

Cummings is a freelance writer in North Andover, Mass. She can be reached at jocummings@comcast.net.

How to staff a SOC

Don't give staffing issues short shrift as you plan your enterprise security operations center, pioneers advise.

Staffing a security operations center can be almost as challenging as building it or paying for it, users and experts say.

The 24/7 monitoring necessary in a SOC presents one of the biggest hurdles. "For companies used to having security personnel working eight hours a day, five days a week, that dramatically increases their overall staffing requirements, since one 24-by-7 seat is equal to roughly five full-time employees," says John Summers, global director of managed security services at Unisys.

Faced with such a prospect, many organizations look to cut corners.

For example, some make the mistake of staffing their SOC solely with their best security personnel. "Companies take seasoned security professionals, stick them in front of a screen and ask them to do a six-hour monitoring shift," says Andreas Antonopoulos, senior vice president and founding partner at Nemertes Research. "You won't retain those people too long because they will very quickly become bored."

Beyond boring and overworking a valued staffer, this tactic also could create a huge security vulnerability.

"If one person is writing your security policy, implementing your policy, monitoring it and then checking for compliance, that person is basically one huge risk," Antonopoulos says. "There's no separation of duties, and absolutely no checks and balances."

Instead, a good SOC, like a good, traditional network operations center, should be staffed in tiers, with Tier 1 personnel receiving alerts and doing low-level troubleshooting and Tier 2 and 3 people handling more complex alerts and problems. In the best of all worlds, Tier 1 personnel should provide the first line of response for both the security and network operations sides of the house.

That way, your more veteran security professionals can handle the more complex risk-management and policy-writing tasks, while putting lower-level staffers into the SOC for the primary monitoring. Then, when alerts come up and the Tier 1 staffers are unsure how to proceed, they can kick up the problem to a Tier 2- or 3-level person. Only then does your more expert, and expensive, staff get involved.

— Joanne Cummings

Worrying about viruses and unwanted content can hold you back. That's why thousands of companies across the globe – from Fortune 100 organizations to small businesses – rely on Sybari to secure their information workplaces, including e-mail, instant messaging, and document sharing.

Our unique solutions use multiple virus scanning engines and industry-leading antispam and content-filtering technologies to stop threats before they stop your business. Make the move to Sybari... and experience the freedom of security and productivity.

Sybari

SECURING THE INFORMATION WORKPLACE

To learn more,
visit **www.sybari.com/nw05**

Taking on Web services with resolve

Visa takes Web services outside the enterprise to streamline the charge-dispute process.

■ BY BETH SCHULTZ

With a corporate ad slogan extolling "It's everywhere you want to be" and a payments network that indeed serves nearly every country in the world, you can bet Visa U.S.A. IT executives feel the onus of availability and reliability.

Hiccups simply can't be tolerated when 14,000 financial institutions count on your payment-processing system for more than $1 trillion in annual transaction volume. That's 5,546 payment-transaction messages per second, or 100 million transactions a day, on average. (During the most recent December shopping frenzy, Visa's message gateway handled 9,200 transaction messages per second.)

Placing that volume in context can be difficult, says Sara Garrison, senior vice president of network and open systems development at Visa, in Foster City, Calif. But think about this, she says: "If you take all the transactions across all the stock markets and exchanges in the world, and you aggregated them over a 24-hour period, we do that volume over a coffee break."

Needless to say, Visa doesn't make infrastructure decisions lightly. But the company does push boundaries and rapidly adopts technologies that could benefit Visa member banks, the merchants they serve and, ultimately, consumers holding the 458 million Visa-branded cards in the U.S. This doesn't mean the company embraces technologies on the high-risk bleeding edge, Garrison says. But it usually finds itself on the leading edge — which makes it well worth watching as it ventures into use of new data center technologies.

Take Visa's evolution toward a services-oriented architecture (SOA) and use of Web services. Like many companies, Visa has long recognized the inherent value of services-centric application development. But Visa leapt ahead of most companies by extending Web services to business partners.

As of late last year, Visa uses Web services to allow direct communication between its back-end systems and those at member banks involved in the charge-dispute process. Visa already used Web services internally for this industrial-strength dispute management system, called Resolve OnLine. A mammoth undertaking that involved 150 developers working concurrently for nine months to meet the first release date, this industry-reference Web application for development projects is now in its fifth-generation release. Created by Visa developers using Java 2 Platform Enterprise Edition (J2EE), Mercury and Rational tools, in conjunction with IBM's WebSphere Integrated Application Suite, Resolve OnLine automates the dialog across back-end systems so disputes could be quickly resolved, Garrison says. Extending Web services to member banks enabled Visa to streamline the process further.

Prior to Resolve OnLine, which went into production in June 2002, cardholder disputes had to be processed on paper. Visa couldn't easily automate the process because of the differing back-end systems and legacy specialized-functionality tools in use throughout the industry. By using Web services, Visa and member banks have eliminated many of the remaining manual processes involved in dispute management. For example, back-end systems at Visa and member banks now can communicate directly regarding requests for transaction research, dispute case search and retrieval, and requests for copies of original paper receipts. Visa secures the inter-enterprise Web services transactions via Secure FTP sessions over SSL.

Since implementing Resolve OnLine, not only has dispute transaction length been reduced but also the number of disputes has diminished. "The inquiry capabilities have lessened the number of issues that come to dispute, and we have seen resolution time cut roughly by one-third," Garrison says.

In 2004, Resolve OnLine saved issuers $52 million in operating costs, while member savings from the reduction in volume of exception items exceeded $300 million during the year, she says.

This Web application is a natural extension of Visa's open systems goal of ensuring that code can be "componentized, encapsulated, compartmentalized, replaced and reused" easily, Garrison says.

Visa readied itself for a Web services SOA by building applications out of self-contained piece parts, and using J2EE to ensure independence from back-end hardware and operating systems. Following best-practices guidelines to ensure scalability, robustness, security and extensibility also has helped. For example, Visa has embraced the Open Management Group's Unified Modeling Language and IBM's Rational Unified Process for configurable software development and automated testing of code.

"We're seeing viable reuse, leading to rapid product delivery," Garrison says, citing development of an Internet file gateway service in three months as one example. Almost half — 47% — of components used for that service came from the Resolve OnLine code base.

Visa now uses Web services in its new application development projects. Already, about 10% of Visa's internal applications have Web services components, Garrison says, and continued extension outward is an absolute must. ■

PHOTO: BOB ADLER

SECURE®
COMPUTING

We triple-dog-dare you.

Trojans, worms, viruses, and application attacks don't scare the all-in-one Sidewinder G_2® Security Appliance. It scares them! It detects and stops them. It protects thousands of networks all over the world and it can protect yours. It includes the world's strongest application-layer firewall that has never been compromised. You can even add optional anti-virus, anti-spam, e-mail and Web content filtering, SSL VPN, and more.

For a free evaluation, call 1 800 379-4944.

New Security Assessment Report Available! *Read Black Hat Consulting's Security Assessment Report on the Sidewinder G_2 Security Appliance. This report details how this appliance handles real-world attack methodologies, ranging from layer two to layer seven attack methods as referenced against the OSI model. Visit* ***www.securecomputing.com/goto/blackhat***

SIDEWINDER G_2® SECURITY APPLIANCE

Firewall/Security Appliance
Sidewinder G_2® Security Appliance
Sidewinder G_2® Enterprise Manager

Strong Authentication
SafeWord® RemoteAccess™
SafeWord® RemoteAccess,™ Cisco compatible
SafeWord® PremierAccess®
SafeWord® for Check Point
SafeWord® for Citrix® MetaFrame®
SafeWord® for Nortel Networks

Web Filtering
SmartFilter,® Sentian,™ Bess®

www.securecomputing.com

COMMON CRITERIA
EAL4+ CERTIFIED

Securing the connections between people, applications, and networks™

All trademarks used herein belong to their respective owners

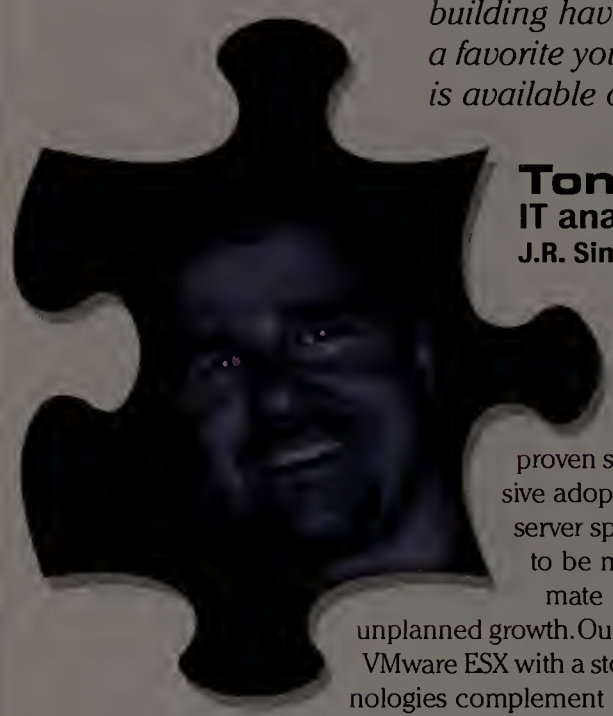
YOUR OPINION

Tech talk

Four IT executives discuss their favorite new data center technologies.

BY JULIE BORT

In the first of an ongoing user discussion series, four IT executives shared their thoughts on hot new data center technologies. They all agree that the flexible new infrastructures they're building have a major upfront benefit — lower total cost of ownership — and each suggests a favorite young technology. A snippet of the conversation appears here; the full version is available online at www.nwfusion.com, DocFinder: 5925.



Tony Adams
IT analyst
J.R. Simplot, an agribusiness firm in Boise, Idaho

Virtualization of servers and storage are our two most significant infrastructure initiatives. Both have been underway for more than a year and have proven successful enough to warrant more aggressive adoption. We have to reduce our accumulated server sprawl and prevent [more] sprawl. We have to be more flexible, and virtualization is the ultimate protection against initial sizing errors or unplanned growth. Our Intel server virtualization strategy is 100% VMware ESX with a storage-area network (SAN). These two technologies complement each other so well that we consider their adoption to be co-requisites. We also must have a seamless disaster-recovery capability. ESX with a SAN-to-SAN remote mirror is a great disaster-recovery strategy for us.

Carmine Iannace
Manager, IT architecture
Welch's, a grape-juice manufacturer in Concord, Mass.

At Welch's, the extended enterprise already is incorporated into our business model and, to a degree, in our IT systems. We currently use a combination of Plumtree Enterprise Portal, Oracle and a number of business intelligence tools [such as Noetix] to collaborate with our partners and produce unique, up-to-the-minute views of sales and marketing data. In the next 18 months, we plan to allow our strategic partners not only to view but also to participate actively in live business transactions in an interactive manner.

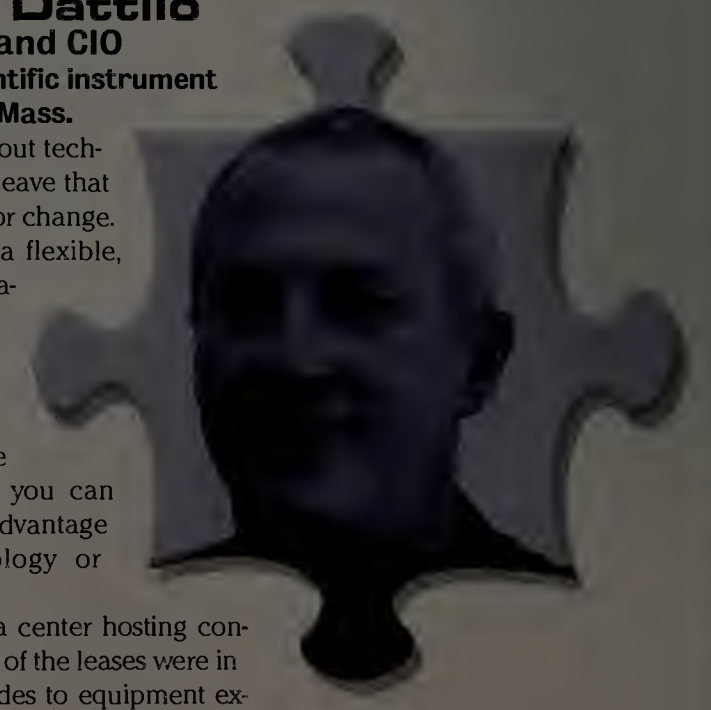
Grid computing is an interesting concept and might hold great promise in the near future. Grid infrastructure is possibly the next logical step in what I believe is the overall commoditization of the corporate data center. Companies that do not embrace commodity servers, virtualization and grid computing and related technologies will not be able to effectively compete because of high operational costs and poor flexibility.

Wireless technologies such as RFID will increase the speed and effectiveness of order and inventory tracking in manufacturing facilities and warehouses. We will see a great increase in the use of short-range wireless technologies akin to Bluetooth and ultra wideband. Forget about the 'last mile' — it's the final 10 or 20 feet.

Rael Paster
Head of collaboration services information technology
Serono, a biotechnology company in Geneva

Anything that can be done to simplify the architecture, while making it more scalable and robust with fewer machines, network ports, back-up devices, CPUs and [operating system] licenses, adds up to a lower overall TCO. Automated systems that will self-heal would be Utopia [and similar to what we've enjoyed on the IBM pSeries and iSeries platforms with a processor failure detection, for example, and continuity of service when this occurs].

Application front-end processors [AFP] greatly enhance the use of existing resources. [With an AFP, you can] offload server I/O, [perform] data compression, multiplex client session requests, and [optimize] Web applications. We've seen our server requirement decrease with AFPs and the WAN and VPN bandwidth requirements drop dramatically [in some cases, to as much as a one-ninth of the traffic]. Network-attached processing, or compute pools for portals and application servers, is a very interesting emerging technology for performance management, and worth watching.



Matthew Dattilo
Vice president and CIO
PerkinElmer, a scientific instrument maker in Wellesley, Mass.

We've talked a lot about technology, so I'm going to leave that alone and focus on planning for change. When we think of designing a flexible, efficient and cost-effective infrastructure, we really need to think in terms of opportunities to enact change and to implement strategy. If you don't do a good job aligning things like leases and service contracts, you can find yourself unable to take advantage of developments in technology or price/performance.

An example would be a data center hosting contract that ran out in 2003, but all of the leases were in effect through 2004, and upgrades to equipment extended beyond the base equipment's lease term. In this scenario, you either lose flexibility, or pay a premium to implement change. You might have accepted the lowest cost alternative for each transaction, but the total cost picture has [not] been optimized.

Scott hates us.

And our customers couldn't be happier. Scott's a hacker and it's our job to make his job impossible. We're Sophos, a global leader in network security.

Over 97,000 viruses want inside your network. The number is growing—and so is the severity of attacks. Sophos knows how to stop them. Join the 25 million business users in 150 countries who already depend on our proven anti-virus, anti-spam and email policy enforcement solutions and acclaimed customer support to protect against multiple evolving threats.

FREE expert resources and the chance to WIN a Dell™ Pocket DJ at stopthethreat.com. Learn how a proven multi-tier network security solution addresses your network's protection, performance, productivity and policy enforcement challenges. Download free white papers, analyst reports and webcasts from independent expert sources at **stopthethreat.com**. While you're there, enter for your chance to win one of two Dell Pocket DJs ($199 value each).

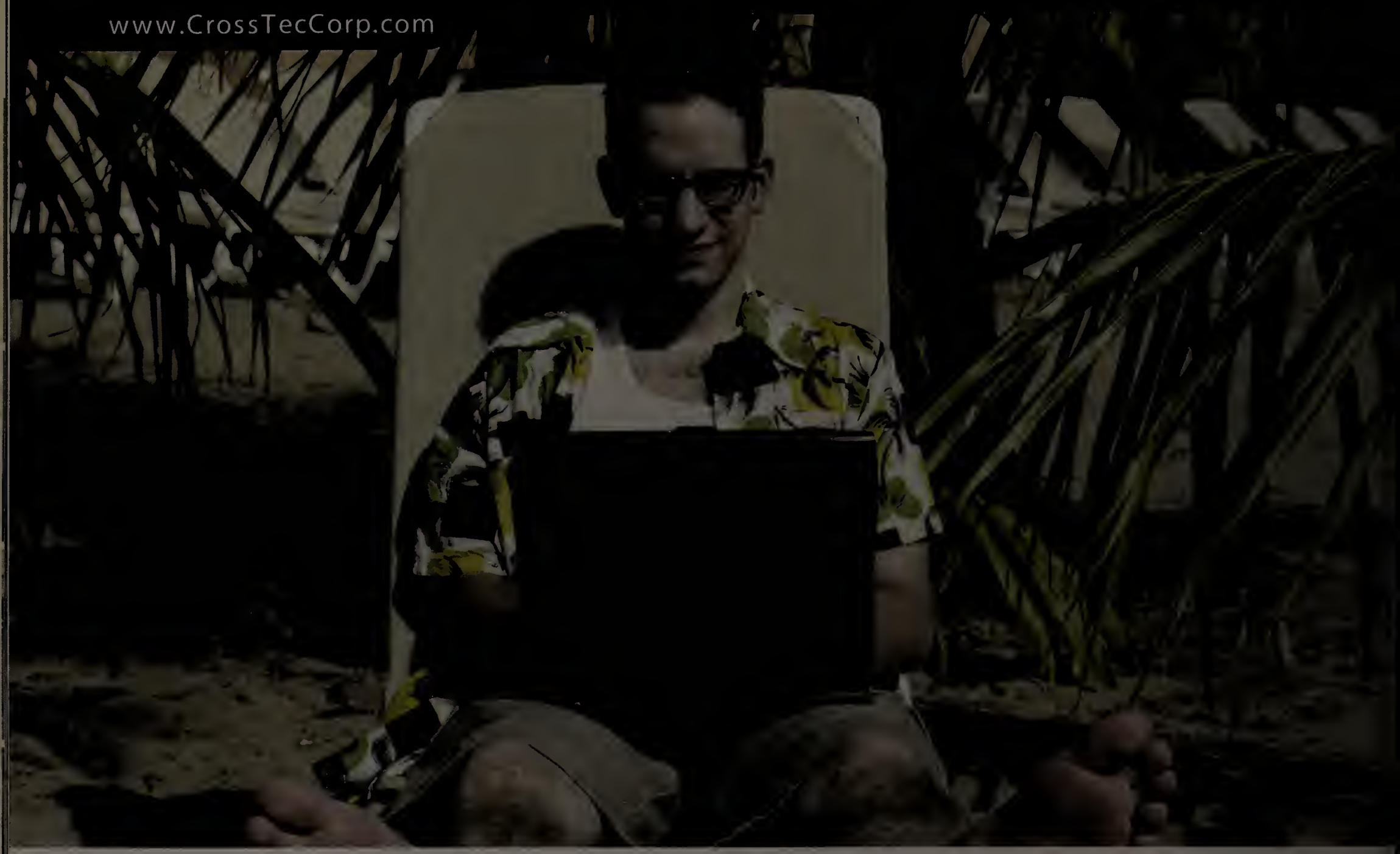
SOPHOS

anti-virus, anti-spam and
email policy for business

Free downloads and the chance to win at **stopthethreat.com** **ENTER PIN: ejm2xza**

NetOp® Desktop Firewall

www.CrossTecCorp.com



Jimmy had a fantastic vacation. Unfortunately, his laptop picked up a tropical disease.

No Problem!

Introducing the world's first 100% driver-centric desktop firewall with centralized control

You know the story – Jimmy's working in an unprotected network environment. Maybe a hot-spot at a café or airport. He checks his e-mail. He does a little recreational surfing. And his laptop is open to attack. But, hey, the risk is minimal...right?

Now, you don't need to worry. The NetOp Desktop Firewall provides all the benefits of both personal and corporate firewalls in a single, powerful package to shield your laptops and network PCs. Not only does NetOp prevent unwanted or dangerous data from entering or leaving your laptops – wherever they happen to be – our centrally managed process control ensures that only authorized programs and services can run on your system. In short, NetOp expects the unexpected!

But we wouldn't want you to take any risks. So try it yourself, absolutely free! You'll find full details at **www.CrossTecCorp.com**.

- Centrally manage and control security policies
- Driver-centric security is always on - even before you receive a network connection
- Intelligent Network Detection switches security policies when you switch networks
- Kill unknown processes before they start
- Stealth ports, Advanced event logging, Block all network access & More

FREE

Download a fully-functional trial copy at www.CrossTecCorp.com

CrossTec Corporation | www.**CrossTecCorp**.com | 800.675.0729

NetOp Desktop Firewall

© Copyright 2000-2005 Danware Data A/S. All rights reserved. NetOp and the red kite are registered trademarks of Danware Data A/S. Other brand and product names are trademarks of their respective holders.

From the makers of award-winning NetOp Remote Control & NetOp School

© 2005 Raritan Computer, Inc. Raritan is a registered trademark.

www.TheMotherOfAllAlarmStorms.com

A fun and informative site for anyone who's ever been in the data center when the bells start ringing.

Securely access and control your IT infrastructure with solutions that simplify and accelerate incident response, service restoration, problem diagnosis and repair – helping to reduce complexity, MTTR and downtime, while improving productivity, flexibility and ROI.

Raritan®

When you're ready to take control.

THE LAST PIECE

When trust isn't enough

Internet expert K.C. Claffy talks about next-generation security architectures.

■ BY SANDRA GITTLEN

K.C. Claffy, a well-respected member of the computer science research community, has made it her mission to understand the Internet and all its nuances. As principal investigator at the Cooperative Association for Internet Data Analysis (CAIDA), an 8-year-old collaboration among commercial, scientific and government entities, Claffy watches over the Internet — collecting and analyzing performance statistics in order to help create an Internet robust enough to handle ever-increasing resource demands. For instance, with Claffy leading the way, CAIDA is the go-to organization for information on 'Net-based virus attacks. In this interview, Claffy, one of our 50 most powerful people in networking for 2004 (www.nwfusion.com, DocFinder: 6321), talks about security on the Internet and in the next-generation enterprise network.

In your time at CAIDA, what Internet performance trends have you noticed?

Consumers and producers in the IT marketplace have gotten used to Moore's Law and expect similar advancements in every product area. Combine the push for more/better/faster with globalization and commoditization and you get the happy result of 10 Gigabit Ethernet selling for the same cost per port in 2005 that 10M-bit/sec Ethernet sold for in 1985. At this point, the challenge isn't getting enough but rather keeping it long enough to depreciate it. Eventually, we'll reach a saturation threshold where a vast majority of powered devices are stagnant. For example, a TCP/IP controllable light switch in your home will send about 10 bits a minute, but because of cost-per-port issues it will be connected by a 54M-bit/sec wireless or 100M-bit/sec wired Ethernet. Upgrades will not be possible.

What changes have you seen in how Internet security is handled?

The greatest single advance has been in "up leveling," the training and salary of law enforcement personnel responsible for managing information-age crime. Ten years ago, anyone who knew how to track down a child pornographer could make a ton more money in the private sector than in the public sector. Today, these skills are taught at the community college level and just about every new FBI special agent is an expert before he gets his badge. This is good, but it's still only the tip of the iceberg. Inter-governmental cooperation, treaties and research funding for information-age affairs is still tiny compared to, for example, what's done with atomic power or space exploration.

Do you see any performance and security problems that can't be solved?

If some day we do all we can — which we're not, today — we'll still be left with human nature. Smart, motivated people will continue to find ways to break laws that haven't been invented yet, and cause law enforcement and the technology industry to innovate to keep up. It's possible that as an evolutionary force, this is good, since it ensures that complacency can't happen.

How will the increasing "Webification" of applications and use of Web services affect Internet performance and security?

As a ubiquitous interface, the Web will make it easier for more attackers to try to guess more passwords. This will look, at first, as though the Web is less secure than the proprietary interfaces it replaces. However, the real weakness is in having guessable passwords, or in having passwords at all rather than hardware-token security schemes (like ATM cards and PINs). Hopefully, the end result will be a rapid advance of the hardware-token security business. Imagine something like Microsoft Passport but not controlled by any one bank or any one software company, but rather by a federation.

What advice would you give to IT executives at Fortune 500 companies that are moving quickly to provide Web-based application access to an ever-widening user base?

I would warn them against single-vendor solutions. Even though multiple vendors are more expensive to manage and deploy, modern enterprises have to have diversity as a core value and management of diversity as a core strength. Follow standards, but get your file servers and desktop clients from different vendors. Both hardware diversity and software diversity is necessary.

What will security look like for the fully automated, virtualized, on-demand enterprise of the future? How will that be different than today's security architecture?

Today's security architecture is a hodgepodge of proprietary systems with various high priests and sole sources keeping it all running. In the future, we'll see single sign-on based on RFID and presence and PINs, retinas, fingerprints, smartcards and other hardware-token schemes. The time is coming when employees will use the same card key to get into the parking lot and the intranet Web server. When they get home and do their Christmas shopping online, they'll be using an RFID-enabled "credit card" plus a USB thumbprint scanner to authorize credit and debit transactions. The reason we don't have this today isn't that it hasn't been invented yet, but that no one trusts any single company to bring it to market, and the federation of related companies and governments for this hasn't been formed as yet.

What's your security advice when it comes to building new data center architectures?

It's 'motherhood and apple pie' time. Security doesn't depend as much on the quality of your locks or firewalls as it does on the usability of the secure system. If you put a man-trap on your data center requiring a 30-second entry/exit process, what you'll get is the back door propped open so that your technicians can go for a smoke when they want one. Similarly, if you put in a firewall so tight that most things can't get through it, what you'll get is a bunch of employees using public 802.11 wireless networks to get the part of their work done that your firewall doesn't allow.

Gittlen is a technology editor in Northboro, Mass. She can be reached at sgittlen@charter.net.

CONSTANT.
CONTROL.

WITH THE DS SERIES, YOU ARE ALWAYS IN CONTROL.

Local data centers. Remote offices. Branch locations. They are all within your reach. The company who invented KVM over IP just made it better.

No more trips back to the office. With the all new DSView® 3 software, you can control servers and serial devices from a single browser interface – you can even power cycle or watch the servers reboot. Since we load balance user authentication for multiple sites, you get faster performance and quick access.

You know, you might even be able to take lunch. For a virtual tour of secure, smarter switching from Avocent, go online to www.avocent.com/control or call 1-866-286-2368.

Avocent

The Power of Being There.

Avocent, the Avocent logo, DSView and The Power of Being There are registered trademarks of Avocent Corporation. Copyright © 2005 Avocent Corporation.

Can your network transform your business?

EVOLVE AT WILL. Can your network turn a tight race into a commanding lead? Can it move quickly into global markets, help drive down costs and be nimble in the face of changing competition? Can it offer both ultra-flexible IP-VPNs and business continuity services? Can it deliver innovative security and IP management expertise? With networking solutions from AT&T, you can integrate your entire value chain into a single, globally networked community. So not only will your enterprise be able to reach the entire world—it might even be capable of changing it. **CAN YOUR NETWORK DO THIS?**

AT&T

The world's networking company℠

To find out how AT&T's networking solutions can help evolve the way you do business, go to:

att.com/transform

©2005 AT&T

Service Providers

■ THE INTERNET ■ EXTRANETS ■ INTEREXCHANGES AND LOCAL CARRIERS
■ WIRELESS ■ REGULATORY AFFAIRS ■ CARRIER INFRASTRUCTURE DEVELOPMENTS

Sprint boosts wireless data services

Extended Workplace provides unified look at remote-access options.

■ BY DENISE PAPPALARDO

Sprint announced last week at CTIA Wireless 2005 that it's beefing up its wireless services for business users.

The carrier launched its Extended Workplace remote access platform. Sprint briefly talked about the service earlier this month. Extended Workplace offers business users a secure platform to access their corporate VPNs via Sprint's PCS Vision wireless data service, dial-up or Wi-Fi.

The carrier teamed with service provider Fiberlink, which also offers secure remote-access services to business users, to develop a single, secure client that lets users see all their access options as they travel around the globe.

Sprint's wireless SLAs

The carrier is the first to offer performance guarantees for both voice and data services.

	Calls that cannot be completed	Calls that end prematurely	Network availability
Wireless voice SLA	Fewer than 2%	Fewer than 2%	99.9%
Wireless data SLA	Fewer than 2%	Fewer than 1%	99.5%

PCS Vision is available across the U.S., and Sprint has a network of 14,000 Wi-Fi hot spots.

Although the service doesn't include wired Ethernet locations such as those offered with remote-access services from competitors AT&T and MCI, there will be future releases of Extended Workplace that likely will include additional access options, says Barry Tishgart, senior director of product management at Sprint.

The service is available for $120 per month, per user, for unlimited PCS Vision and Wi-Fi access. While the plan includes dial-up, users pay for that service based on how much they use. Users will pay 35 cents per hour for local dial-up, $2.95 per hour for toll-free dial-up and $1.40 per

See Sprint, page 64

IETF eyes 'Net emergency communications

System would route urgent calls over Internet much as 911 telephone network does now.

■ BY CAROLYN DUFFY MARSAN

The IETF has kicked off an effort to develop communications protocols needed to support emergency communications over the Internet.

The new IETF working group is called Emergency Context Resolutions with Internet Technologies (ECRIT). ECRIT is looking for a way to route emergency calls over the Internet similar to the way in which 911 calls are routed over the public switched telephone network (PSTN).

If successful, ECRIT would have a significant effect on service providers, including traditional wireline and wireless carriers, ISPs and start-up VoIP providers, because they would need to upgrade network hardware and software to support any new system.

Universal standards

"The ambition of this working group is to provide a universal solution for a particular part of the emergency communications problem," says Jon Peterson, an engineer with NeuStar who serves as the Transport Area director overseeing ECRIT. "We are looking at how, based on the context of an emergency call, to route it to the right emergency call center."

ECRIT is not addressing prioritization or pre-emption of emergency calls, which is available in many government and military telephone systems. Instead, the IETF's Internet Emergency Preparedness working group is handling those issues as it develops an overall architecture for communications systems used for disaster recovery.

"We're looking at the consumer, 911-class problem over the public Internet," Peterson says.

Because it addresses this broader need, "ECRIT is the most important protocol work going on in the IETF related to emergency communications," he says.

The IETF announced the ECRIT working group in February, and ECRIT held its first meeting March 9 in Minneapolis.

The PSTN has been configured to recognize specific numbers such as 911 or 112 as calls for emergency services. These calls are sent to special call centers that handle emergency response. These emergency calls are associated with the physical location of the call originator so they can be routed to the appropriate emergency call center.

With its many overlay networks and tunneling mechanisms, the Internet is a more challenging infrastructure for building an emergency communications system than the PSTN, IETF participants say. The ECRIT working group is trying to define the requirements of Internet-based emergency calling and to select appropriate technologies for describing the location of the call originator and managing the call routing.

Video, text messaging service

ECRIT is focused on VoIP calls, but the

See IETF, page 64

Short Takes

■ **AT&T** said last week that it is planning to test **WiMAX technology** with two unidentified customers beginning the first week of May. WiMAX, the IEEE 802.16 specification, is a last-mile wireless technology that uses the 700-MHz to 66-GHz frequency to deliver transmission speeds from 2M to 6M bit/sec. This is AT&T's first WiMAX trial. AT&T says it hopes to use the technology to lower its access costs paid to local exchange carriers; AT&T says it pays $8.5 billion per year to LECs. The company expects to offer wireless last-mile services next year but has not mentioned how its pending merger with SBC might affect its plans. The two customers testing the WiMAX service are based in Middletown, N.J., near AT&T's headquarters.

■ **Equant** announced last week that it has inked two deals totaling $2.3 million with **Ampacet,** a chemical compound manufacturer in Tarrytown, N.Y. The first is a three-year contract to deploy and manage an IP VPN. The second is a two-year contract to manage its messaging infrastructure. Equant has deployed 14 nodes on Ampacet's global network in North and South America. Ampacet is expanding its relationship with Equant to add Ampacet's corporate locations in Asia and Europe to its IP VPN network.
Ampacet previously had frame relay services from Sprint, but after billing and network performance trouble, the company said it decided to choose a new provider. After talking with several global service providers Ampacet says it selected Equant because the carrier had real network presences in all the countries where it needed services.

More online

Read more information on the ECRIT working group.

DocFinder: 0335

EYE ON THE CARRIERS

Johna Till Johnson

Ebbers verdict: Comeuppance, without glee

The Germans seem to have a word for everything. *Schadenfreude* is usually translated as "glee over another's misfortune." And it's how I expected to feel when the news came down last week that a New York jury found Bernie Ebbers guilty of conspiracy and eight counts of accounting fraud.

Guess what? I'm not feeling gleeful. The closest way to describe how I feel is relieved. Relieved because 12 ordinary New Yorkers actually get it: It's not OK to lie, cheat and steal your way to success. And it's not OK to let others do your dirty work and then argue that because you didn't understand the details you should be let off the hook.

The value of a guilty verdict, in many cases, isn't the ability to deter future criminals or cause current ones to suffer. It's a way we as a society associate a comeuppance with a crime, and by doing so, define who we are and what kind of people we want to be. By saying certain behavior merits punishment, we're also defining what kind of behavior we expect and demand from our citizens.

Telling the truth and taking responsibility for our actions are two of the values that were reaffirmed last Tuesday. So I'm relieved that at least some of us still know right from wrong and believe in accountability and personal responsibility.

That doesn't mean last week's verdict is a happy event. Convicting Ebbers doesn't return the $11 billion to shareholders who lost their life's savings. It doesn't return jobs to the thousands of MCI and WorldCom employees who lost their livelihoods. It doesn't resuscitate the trashed careers of the executives at other telcos who had to compete with fraudulent performance and cooked books. Sending Ebbers to the slammer just adds one more damaged life and family — his — to the thousands his actions left in their wake. No, this conviction is not an occasion for glee or even quiet rejoicing.

But it is a good reminder to take a minute and review our fundamental beliefs — the standards of behavior that we expect and demand from citizens, and the violation of which become grounds for prosecution.

Here are mine:

- Leaders (whether senior executives at for-profit or not-for-profit organizations, politicians or their appointees, or military officers) assume responsibility for defining and living up to a high ethical and legal standard. They set the example for every individual in their organizations.

"I didn't know" isn't an excuse for leaders. It's your job to know — if you don't, step down and ask someone else to lead.

- Trust is an essential commodity that must be earned on an ongoing basis, by telling the truth and living up to your word — and when necessary, admitting and making reparations for errors.
- CEOs of public companies need to remember that they're stewards of the public trust. If they want glamour, glory and limited personal responsibility — they ought to become actors or rock stars. Maybe Ebbers should have stuck to coaching basketball.

Johnson is president and chief research officer at Nemertes Research, an independent technology research firm. She can be reached at johna@nemertes.com.

IETF

continued from page 63

group's charter says it also will consider the use of video or text-messaging communications to request emergency services.

Hideki Arai, an engineer with the Oki Electric Industry in Japan, said the new system "must be equivalent to traditional emergency calling ... and it must be easy to migrate from the PSTN to the Internet."

Arai briefed the working group on an ongoing Japanese government effort to outline its own requirements for emergency calling with IP telephony services.

Brian Rosen, president of start-up Emergicom, says the Internet emergency calls also need to be traceable in case something goes wrong. "You need to know what happened to a call," Rosen says. You also need a call-back mechanism in case the caller hangs up, he adds.

Challenges loom

Participants in the ECRIT working group agree that building an Internet-based emergency communications system is a challenge.

"One of the hardest things is how much do we worry about being backwards compatible," said Henning Schulzrinne, a professor of computer science at Columbia University who outlined several requirements for emergency calling using Session Initiation Protocol.

The ECRIT system also needs redundancy and reliability.

"You need to have congestion control everywhere because when bad things happen lots of people make emergency calls," Rosen says.

The ECRIT working group seems to favor using protocols developed by another IETF working group called Geographic Location/Privacy to fetch and deliver location information to its emergency call routing system.

The Internet's 911

Core requirements for an Internet-based emergency communications system include:

- Identifying and validating emergency calls so that all carriers along the call path know it is an emergency call.
- Determining the location of calls.
- Routing calls to an appropriate emergency call center.
- Protecting against spoofing.

The ECRIT working group's first milestone is to develop a document that defines the terminology involved in emergency communications over the Internet and lay out the requirements necessary for the system. The group says it hopes to have this document completed in April.

After that, the working group has set an aggressive timetable for its work. It plans to complete a document outlining security considerations in April. By August, the group intends to complete three documents: one on setting up communications sessions between callers and emergency response centers; another on associating sessions with physical locations; and a third on routing emergency calls based on location information.

Peterson says he's optimistic that ECRIT can meet its schedule. "At the meeting, we had many different groups presenting that represented Japan, Europe and North America, and they all outlined the same core requirements," he said. "That was very heartening." ■

ISP News Report
Subscribe to our free newsletter.
DocFinder: 5434 www.nwfusion.com

Sprint

continued from page 63

hour for domestic roaming off of Sprint's network.

First wireless data SLA

Sprint also announced at the show the first wireless data service-level agreement (SLA).

Last summer Sprint became the first wireless service provider to offer an SLA for its mobile voice services for business customers (see www.nwfusion.com, DocFinder: 6336).

Sprint's wireless data SLA guarantees 99.5% network availability, and that wireless data blocks will be less than 2% and wireless data drops will be less than 1%.

If the carrier misses these, metrics users are entitled to a 10% credit of their wireless data monthly recurring charge. In other words, if a company pays $1,000 per month for all of its wireless data services it will receive a $100 credit.

The credits are not proactive. Users must log on to a secure Sprint Web portal to view the carrier's monthly network performance statistics. If Sprint didn't meet its SLA, the user then has to request a credit.

"It's not the type of feature that's going to get customers to sign deals," says Bob Egan, president of consulting firm Mobile Competency. But more business users interested in Sprint services might call the carrier to get information, he says.

One drawback of the SLA is that users are required to have someone internally manage and monitor it, Egan says. Every month it's that person's responsibility to check the Web site, request a credit from Sprint if necessary and follow up on those requests.

"It requires resources that some users may not have," he says.

Sprint's Tishgart points out that this is Sprint's first wireless data SLA and that it plans to continue to improve on the particulars of the guarantee.

The carrier also announced the general availability of its Sprint Managed Mobility Service (DocFinder: 6337). SMMS is a management tool that provides rate optimization, over-the-air software upgrades, security features and asset management features.

Imagistics, a document management company, started using the service in October last year as it was upgrading all of its employees' Treo wireless devices. Initially the Trumbull, Conn., company used the tool to replace about 1,000 Treo 300s with Treo 600s.

"Sprint managed the deployment without a hitch," says John Chiliock, vice president of customer service operations at Imagistics. "I could not have technicians in the field with devices that weren't running."

Imagistics used the service and procurement piece of the SMMS service, which falls under asset management, to upgrade its employees' devices. It is also using the security features, which include zapping phones remotely if they are lost or stolen, rendering them useless in the hands of a thief; and erasing corporate data. The company also uses the billing tools that let it ensure its pooled minutes plan meets the company's needs, he says. ■

www.nwfusion.com
More online!
Explore options in local- and wide-area wireless data services. And discover strategies that implement mobile applications effectively. Attend Wireless & Mobility: Commanding Broadband Everywhere — a new Tech Tour and Expo event coming to a city near you.
DocFinder: 5839

VIRUSES CAN REPLICATE 1,000 TIMES A MINUTE.

How fast can you install a patch?

Antivirus protection is a never-ending race against time. And the bad guys get faster every day. Good thing Websense software fills the time and technology gaps that existing antivirus and security solutions can't address. **Close the security gap. Download your free evaluation today. www.websense.com/patch5**

WEBSENSE.
SECURING PRODUCTIVITY™

© 2005 Websense, Inc. All rights reserved. Websense is e registered tredemerk of Websense, Inc. in the United States and certain international markets.

LINKSYS®
A Division of Cisco Systems, Inc.

Speed and Range eXpansion

Faster and Farther Than Ever Before!

Wireless-G with SRX

WRT54GX
Wireless-G
Broadband Router
with SRX

Speed and Range eXpansion

Watch streaming video or play multi-player games faster than ever before. And do it comfortably from places that were previously unreachable. Introducing the Wireless-G with SRX series, the newest, fastest, most powerful addition to the Linksys Wireless-G family.

Enjoy the Wireless-G with SRX experience:

- Up to 8 times faster than standard Wireless-G
- Increased wireless range up to 3 times farther
- Reduced dead spots in coverage area
- Compatible with Wireless-G and B networks

WPC54GX
Wireless-G
Notebook Adapter
with SRX

Visit www.Linksys.com/SRX today for product details, or call our Advice Line at

1-800-737-7201

LINKSYS Partner Connection

CDW

STAPLES

that was easy.

Office DEPOT

Linksys is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. Copyright © 2005 Cisco Systems, Inc. All rights reserved.

CISCO SYSTEMS

Net.Worker

■ PRODUCTS, SERVICES AND STRATEGIES FOR TYING TELEWORKERS TO THE ENTERPRISE

MIMO products boost 802.11g nets

■ BY CRAIG MATHIAS

Wireless LANs are a natural fit in the home and, for some, a constant source of fits. Standard 802.11 WLANs suffer limited throughput, which only worsens as the distance between the client and the access point/router increases. The highly variable nature of radio propagation means seemingly short distances can yield poor results, especially when walls and floors get in the way.

To improve conditions and make WLANs robust enough to stream media, hardware vendors have begun applying multiple-input/multiple-output (MIMO) technology. MIMO uses multiple antennas on each end of a radio link to send and receive several unique radio signals in a single radio frequency channel. The ability to send multiple, distinct datastreams over the same signal simultaneously, known as spatial multiplexing, can double and even triple data throughput rates.

Moreover, sophisticated algorithms create a signal that's louder, which translates directly into corresponding improvements in performance.

Belkin entered the consumer market last fall with the first MIMO-based products, built using Airgo Networks' chipset — products Belkin calls pre-N, in reference to the IEEE's upcoming 802.11n standard.

Since last fall, Linksys, D-Link Systems and Netgear have shipped "MIMO-based" products. However, the technologies they use and call MIMO vary considerably. While all three use multiple antennas to send and receive multiple datastreams over the same signal, only the Linksys SRX line uses spacial multiplexing (like Belkin) to transmit multiple, distinct datastreams over the same signal.

These first MIMO-based products won't be compatible with those based on the final 802.11n specification. However, they are fully Wi-Fi-compliant. Three important questions remain: Do today's MIMO-based products provide sufficient performance to justify the cost? How does the performance compare with standard 802.11g products? Do they cause interoperability problems on a mixed network?

To find out, we devised a series of tests to determine how MIMO-based products would fare against standard 802.11g gear. To mitigate the effect of radio-related artifacts, we rented a house for the sole purpose of running these tests. It was empty except for our equipment and us.

To benchmark performance, we used Iperf, a free LAN test suite (www.nwfusion.com, DocFinder: 5852). We ran the same test in each case; the only variables being the devices tested and their locations. Because location can't be reproduced precisely with antenna orientation, we placed the client notebooks on turntables revolving at 45 seconds per rotation. This let each radio cycle pass through a range of orientations, factoring out any overly beneficial (or detrimental) positioning. Two full cycles (90 seconds) defined each run.

We tested two MIMO products, Belkin's pre-N router (F5D8230-4) and PC card (F5D8010); and four standard 802.11g products — the Linksys WRT54GS router and WPC54GS PC Card, and the Netgear WGU624 router and WG511T PC Card. (We turned off the power management on our Dell Inspiron 8600 notebook and used default driver settings.)

The Iperf benchmark ran in three configurations. First, we put the client and router in the same room with 13 feet apart, which served as a baseline. For the second, we had the client on the same floor as the router, 45.8 feet away and three walls between them. For the third, we had the client upstairs, 46.7 feet away from the router, with four walls and a floor between them. We tested all combinations of clients and routers, and examined upstream and downstream performance.

Not surprisingly, the MIMO-based products from Belkin yielded the best throughput and range. In the homogeneous tests (client and router from the same vendor), the non-MIMO configurations had only 41% to 72% of the throughput of the pure MIMO client and router. Moreover, a mixture of MIMO and non-MIMO products yielded better results in every case than a homogeneous, non-MIMO configuration. This shows that MIMO provides a benefit, even when implemented on only one end.

We experienced no interoperability problems — the MIMO gear worked well with all the other equipment. Finally, having MIMO on at least one end of the connection let us establish a link when we couldn't establish a homogeneous connection.

The pure Belkin configuration provided nearly 15M bit/sec of throughput in the upstairs test, where the homogeneous configurations of the other products usually failed to connect at all.

Our interoperability tests put to rest any concerns about the ability of Belkin pre-N products to work with standard 802.11g offerings. The performance improvements with MIMO-based products on only one end of the connection were impressive.

We recommend these first MIMO-based products to residential users. There is significantly better throughput and range performance than conventional products in every case we tested. MIMO-based is a better approach than adding third-party, high-gain antennas or active repeaters — it's less complex and, even with the higher prices, usually less expensive.

Mathias is the principal analyst at Farpoint Group. He can be reached at craig@farpointgroup.com.

MIMO rises to the top

Belkin's MIMO technology outperformed other vendors' non-MIMO equipment (rates are in megabits per second).

Baseline (same room)

Downstairs test (46.7 feet away from router, separated by four walls and a floor)

	Belkin AP	Netgear AP	Linksys AP
Belkin client	14.9	1.7	7.7
Netgear client	1.1	DNC	DNC
Linksys client	5.4	0.1	DNC

DNC: Did not connect

Short Takes

■ **Netgear** has announced plans to develop a **HomePlug** wall-plugged Ethernet bridge and adapters based on Intellon's 85M bit/sec power-line networking chipset. The products will be suitable for high-bandwidth home network multimedia applications such as TV over IP, VoIP and multi-room DVR. Netgear has yet to announce pricing or availability. The HomePlugAV specification, which will provide 100M bit/sec-plus data rates, is expected to be released in June.

■ The **HomePlug Powerline Alliance** has announced it will develop a specification for a low command and control technology that will co-exist with HomePlug power-line technology. The specification will allow for whole-house control of lighting and appliances, and let them respond to simple commands like "turn on" and "turn off" and to report their status to a controller device. Applications will include security and safety monitoring, device monitoring, status reporting and energy management.

Produced by:

trendsmedia

www.wireless-security-conference.com

April 19-21, 2005
Cambridge, MA

Wireless Security
Conference & Expo

Securing Enterprise Wireless Networks and Mobile Devices

"Nearly one out of every two recorded digital attacks are now taking place via the wireless route as opposed to one out every ten, at the start of 2004."

mi2g Intelligence Unit

Do You Have Your Wireless Security Plans in Place?

The only event focused on enterprise wireless security solutions!

Over 25 of the world's top wireless security experts, including:

- Craig Mathias, *Principal, Farpoint Group*
- Iain Gillott, *Principal, iGillottResearch*
- Frank Hanzlik, *Managing Director, Wi-Fi Alliance*
- Dale Kutnick, *Chairman & Sr. Research Advisor, META Group*
- Les Owens, *Mobile & Wireless Security Booz Allen Hamilton*
- Lisa Phifer, *Vice President, Core Competence Inc.*
- Paul Simmonds, *Global Information Security Director, ICI Plc. & Founder, Jericho Forum*

Pre-conference Seminar on April 19: Understanding Wi-Fi Risks and Countermeasures

Corporate Sponsors:

AIRMAGNET
NEWBURY NETWORKS
RAPID
RSA
ROVING PLANET
unicom

Media and Research Sponsors:

America's Network
FierceWiFi
FierceWireless
InfoWorld
Mobile Enterprise
NetworkWorld
SOFTWARE
Wireless
WiMAX Trends
Wireless Workforce Online
SC MAGAZINE
ITtoolbox

Analyst Sponsors:

Farpoint Group
i Research
METAGROUP
RETHINK IT

Endorsed by:

JERICHO
Wi-Fi
LIBERTY ALLIANCE PROJECT
Mass Software Council
mobile ENTERPRISE ALLIANCE
THE TECHNOLOGY COLLABORATIVE

Technology Update

■ AN INSIDE LOOK AT TECHNOLOGIES AND STANDARDS

RFID readers route tag traffic

■ BY MARGARET WASSERMAN

At every turn, networks must handle additional traffic from new sources. One of the latest and soon-to-rise sources of increased network traffic arises from the implementation of radio frequency identification, which is being used for needs such as supply-chain management, tracking airport baggage and prescription medication shipments. These examples alone suggest a growing volume of TCP/IP network traffic and data.

While conventional RFID readers were essentially data radios, today's enterprise-grade RFID tag readers — created specifically for electronic product code (EPC) usage — have been designed to be full-fledged network devices that can support mission-critical operations. In addition to managing a dynamic population of tags, then routing data into networks, databases and business applications, these RFID readers have to speak TCP/IP natively and fully support standard network technologies such as DHCP, User Datagram Protocol (UDP)/IP over Ethernet, 802.11x, HTTP, SNMP and remote upgrades.

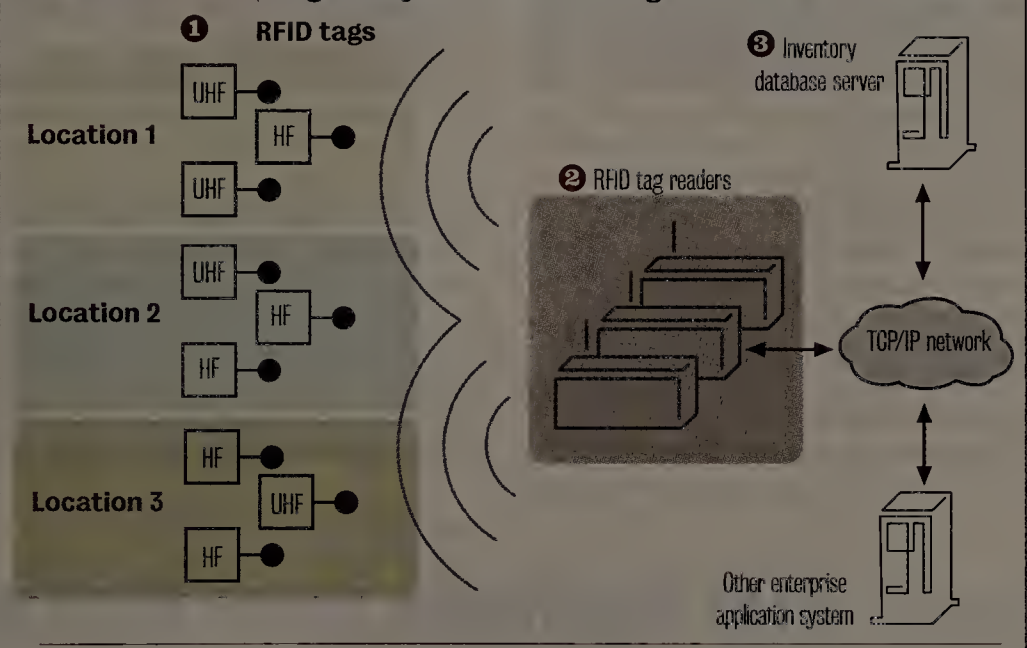
This design lets RFID be widely deployed in an economical, scalable, secure and manageable manner on WANs and LANs, even with the two-way demands of RFID data for networks and changes to RFID tags emanating from within the network.

Driven by speedy network processors and advanced software, RFID readers provide the same load balancing, QoS and security found in high-end IP routers. A tag reader will facilitate advanced applications by acting as a gateway between an IP network and tags that provide read-write data storage, on-board sensors and other features.

■ HOW IT WORKS

RFID tag reader

Radio frequency identification tag readers are designed to be full-fledged network devices that act as gateways between RFID tags and IP-based networks.



1. Large populations of RFID tags are attached to physical objects. The tags move through multiple locations, using either high frequency (HF) or ultra high frequency (UHF) radio signals to communicate with RFID tag readers.
2. The RFID tag readers deal with collisions between tags and extract data from each tag. Typically, this data is the IP address — like electronic product code, which can be used to find networked data associated with that tag. The reader then filters out redundant reads and also may assign prioritization to different identities.
3. Wired or wireless TCP/IP is used to send the extracted data onto a corporate network for processing by enterprise systems such as databases and business applications.

The network gateway functionality of RFID readers becomes even more critical in light of the channel-sharing, data-exchange and air-interface protocols required to accommodate two-way TCP/IP traffic. Before exchanging information with a tag, a networked reader searches for and retrieves the ID of each tag in its read zone. This discovery process produces a list of IDs, which then must be made available to an external software system such as a warehouse management system that resides on a remote networked server.

When the warehouse management system wishes to read, write and update data on the tag, it routes the updated data back to the tag via the reader through which the tag was orignally read. This is analogous to an IP routing procedure in which a reader forwards an encapsulated data packet to a specific tag.

The scenario is clearer in the case of sensor or actuator tags, which typically contain a miniature battery and are used for applications such as time-temperature monitoring of perishable goods in the supply chain.

First, the same networked discovery process applies in the case of sensor tags. Then, bidirectional communication occurs between the tag and software residing on a networked server. In some cases, such as time-critical movement of tagged packages on a conveyor belt, the reader might be given authority to act quickly on a networked server's behalf. This can be accomplished by running specialized software on the reader, or by implementing and populating a policy-based decision-making mechanism, mimicking those employed by high-end IP routers.

The new RFID readers are designed to provide the functionality of a gateway for large networks. RF interfaces to the tags reside on one side of a reader, with a database server and a TCP/IP network interface on the other side, fully equipped to be part of a networked-distributed data aggregation and analysis system.

Wasserman is vice president of development for ThingMagic, serves on the IETF Steering Group and is a member of the Board of Trustees of the Internet Society. She can be reached at margaret@thingmagic.com.

Ask Dr. Internet

By Steve Blass

Is there a way to support Active Server Page documents on an Apache Web server running on a Linux system?

Yes — Apache::ASP, available at www.apache-asp.org, supports ASP on Apache Web servers that use Mod Perl. The package works with Windows and Linux systems. The Apache::ASP program can be installed using Perl CPAN. Start "perl –MCPAN –e shell" to start the CPAN shell interface. At the cpan> prompt, issue the command "install Bundle::CPAN" to update the local copy of the CPAN program. After the update completes, issue the command "reload cpan." Now you can install Apache::ASP by typing "install Bundle::Apache::ASP" at the cpan> prompt. After installing that module, copy the contents of the site/eg/ directory from the Apache::ASP installation directory. Add a <Directory> section to your Apache httpd.conf file, providing "AllowOverride All" privileges for the .htaccess file in the newly created ASP directory in your Apache document tree. Restart Apache after putting the example files (and .htaccess file) in place and you should see the Apache::ASP examples home page. The provided examples include a page hit counter, fill out form samples and XML parsing demonstration code to get you started with programming ASP files that can be delivered from an Apache Web server.

GEARHEAD INSIDE THE NETWORK MACHINE

Mark Gibbs

Back that thang up — some more!

Last week we started with a rant, segued into a review of the IntraDyn RocketVault and wound up talking about the various technologies that underlie the RocketVault. We ended with a discussion of the Common Internet Filesystem.

We're sure many of you were left wondering: "So where is CIFS in the standards process today?" The answer is, sort of floating around. We can't find any specific work on CIFS at the IETF, other than some draft standards that exceeded the six-month limit after which they get dropped. Ho hum.

Despite CIFS being in standards limbo, it is now so widely used and so well understood that it is here to stay. In other words, it is "a good thing" (copyright Martha Stewart).

Anyway, back to the IntraDyn RocketVault. We really like this device. It is a terrific solution for small businesses and branch offices despite a few rough edges.

Installation is simple enough: Connect the RocketVault to your DHCP-enabled network, browse to http://rocketvault/, and log on using the default name and password. Configuration is straightforward.

As we said last week, the RocketVault backs up any files that it can see on any SMB/CIFS network shares to which you care to direct it. You start by defining groups of shares and give each group a combination of daily, weekly and monthly back-up schedules.

With each of those schedules, you also specify a retention period that defines the number of backups that will be kept. For example, if you are configuring weekly backups and you select 12 week retention, then when Week 13 rolls around the back-up from the first week gets deleted.

The various schedules allow for a hierarchy of restore points. For example, you might have daily backups on workdays with a 4-week retention (that is, one month's worth). And you also might have weekly backups performed on a Sunday with a 12-week retention, and monthly backups performed on the first of each month with a six-month retention.

Unlike other back-up systems, the RocketVault doesn't require you to specify whether backups are to be full or incremental — the device determines the best method based upon the number of changed files. The goal is to balance the back-up load so the total run-time of each backup is roughly constant from day to day.

A feature called RemoteVault AES — the AES part signifies that this feature optionally supports encrypting the back-up data using the 256-bit Advanced Encryption Standard — lets the RocketVault also back up any of the defined groups to a remote FTP server.

A gotcha here is that the RemoteVault facility doesn't support passwords for remote servers that contain spaces and special characters, a limitation that might conflict with your system's password policy.

The RocketVault also can be used to synchronize a source and destination at block level in as close to real time as the network and processing capabilities will allow. This feature is called SyncDR and relies on the Unix Secure Shell, SSH and rsync utilities.

We discussed SSH in this column some time ago (see "Secure communications with SSH," www.nwfusion.com, DocFinder: 6338), but rsync is a new topic for us.

According to the rsync home page (DocFinder: 6339), "rsync is an open source utility that provides fast incremental file transfer." To put a little more meat on those bones, rsync implements a remote-update protocol that allows for the transfer across a network connection of just the differences between two sets of files using an efficient checksum-search algorithm.

While rsync can be used locally to make file copies on the local machine, its value lies in copying to and from remote machines. In this role, rsync simply can list the files on a remote machine or, more usefully, copy files in either direction between the local machine and a remote machine using a remote shell (such as SSH) at both ends, an rsync server at both ends, or a remote shell at one end and an rsync server at the other.

You can run rsync on Windows but you first need to install the Cygwin system that we discussed in Gearhead some time ago (DocFinder: 6340). And even then you won't be happy, as we are told that rsync on Cygwin will choke on files larger than 2G bytes. Well, darn.

We'll wrap this up next week. Meanwhile, we're waiting to hear from you at gearhead@gibbs.com. And have you checked Gearblog this week (DocFinder: 6341)? If not, why not?

Cool Tools

Quick takes on high-tech toys

By Keith Shaw

CTIA highlights more than cell phones

Here's a quick look at some of the highlights from last week's CTIA Wireless 2005 show in New Orleans, where the cell phone industry trots out the latest cell phones and other handheld devices that aim to ooh and ahh us through the spring and early summer.

With LG's VX8100 you can view on-demand video clips.

LG showed off its VX8100, successor to the VX8000 phone currently being sold by Verizon Wireless that works on the Code Division Multiple Access Evolution-Data Optimized network and has the ability to view on-demand video clips. The VX8100 phone has all the features of the VX8000 (including a 1.3-megapixel camera with a flash and a camcorder that can record up to 15 seconds of video) with the addition of Bluetooth connectivity and a mini-Secure Digital memory card slot for additional storage. LG and Sprint also announced the MM-535, a phone with a slider design that also includes a 1.3-megapixel digital camera, mini-SD card slot, speakerphone and 3-D sound capabilities. Pricing and availability of the phones was not announced.

LG and Sprint's MM-535 phone features a slider design, digital camera, 3-D sound capabilities and more.

There are always accessory-related announcements at the show, and Bluetooth headsets are always in abundance. Plantronics showed off two new headsets, a premium model code-named Tahiti features an entry-level headset (code-named Tonga) that has up to nine hours of talk time and has an easier way to answer and end phone calls, and adjust the volume (instead of multiple buttons, users press one button to answer/end calls or move it forward or backward to adjust the volume). Plantronics officials say the Tonga headset will cost around $50, making it affordable for first-time Bluetooth headset users. Pricing for premium models usually ranges from $70 up to $150.

Plantronics' Tahiti headset is an entry-level Bluetooth hands-free device.

Sometimes you don't need a cell phone-related product to make a splash at the show. GN Netcom was showing off its GN 9350, a wireless headset that connects to a traditional desktop phone and can be connected to VoIP applications through an integrated USB adapter. With the click of a button on the wireless headset, users can switch from their office phones to VoIP soft phone applications and answer different calls. The company wasn't saying what wireless technology it was using, but said it wasn't Bluetooth because it wants to achieve a range of up to 450 feet in an office environment. The 9350 also includes digital signal processing technology that is designed to help enhance and clean up the incoming signal to help improve call sound quality, GN Netcom says. For example, the headset can monitor and adjust the signal volume on each call (whether it comes from a VoIP connection or a regular analog call) so that users hear every call at the same level. It also features an extendable boom arm and noise-canceling microphone, so it can adjust to the shape of a user's face more comfortably. The device is scheduled to be available in the fall. Pricing was not announced.

The product I got most excited about had no cell phone network attached to it. Research In Motion showed a prototype of its upcoming 7270 handheld, which uses a Wi-Fi connection to provide users with the same wireless e-mail capability they get through a wide-area connection. While some users might scoff at having a Wi-Fi-only connection, this device should be interesting to corporations that have a Wi-Fi network on their campuses. They can have a device that lets roaming employees (not road warriors but those who wander from their desks) keep up-to-date on their e-mail and a VoIP application that lets them make and receive phone calls as if they had never left their desks. More details are promised later this spring.

Shaw can be reached at kshaw@nww.com

Face-off

Is Layer 5 the best place to attack WAN optimization?

Two vendors debate the pros and cons of handling optimization at the session layer.

Yes, by Andrew Foss, Swan Labs

As companies become more distributed and remote workers using bandwidth-intensive applications over the WAN more numerous, the need for better WAN optimization and application acceleration techniques has become glaringly apparent. Most approaches to solving this problem focus on either Layer 3 (the network layer) or Layer 7 (the applications layer) of the Open Systems Interconnection model. However, by combining the best of both of these approaches and then managing traffic sessions at Layer 5 (the session layer), application performance and WAN optimization can reach an entirely new level.

Technologies aiming to solve the bandwidth problem at Layer 3 accelerate all traffic over the WAN by reducing the duplication of data in the datastream as it enters the WAN. These technologies have two key shortcomings: First, they require significant processing resources and, in some cases, actually can slow down traffic. Second, Layer 3 technologies are not aware of the functions of the applications merged into the datastream, so they are unable to speed up traffic for any specific application.

Other technologies focus solely on accelerating the performance of individual applications by compressing data and streamlining protocols at Layer 7. However, because these "accelerated" applications are mixed in with uncompressed WAN traffic, it is impossible to guarantee that the compressed application consistently will perform as required. Also, application-layer technologies only increase the performance of a single application — they suffer a dramatic performance drop-off when working with two or more applications, as they tend to favor the application for which they were designed.

Combining WAN optimization and application acceleration by managing traffic at Layer 5 provides the ability to examine application datastreams before they merge, which finds and removes more redundancies than Layer 3 methods. This eliminates data transfer redundancy by grouping data by session and sending only once, which reduces the number of data roundtrips over the WAN.

By looking at all application datastreams and automatically determining which streams can benefit from compression and protocol optimization, WAN optimization technologies that operate at Layer 5 also can accelerate more traffic types than Layer 7 technologies. And by reusing the compression dictionaries, technologies that operate at Layer 5 greatly reduce the number of needed updates. This optimizes the WAN connection for ROI while guaranteeing the behavior of networked applications under a variety of WAN conditions.

The volume of enterprise WAN traffic continues to grow as applications become ever more sophisticated, and the old rules can no longer handle this new, speedier data flow. By converging application acceleration with WAN optimization and managing it at Layer 5, WAN optimization products let applications used over the WAN experience true, LAN-like performance.

Foss is CEO of Swan Labs, an enterprise application company. He can be reached at afoss@swanlabs.com.

No, by Jef Graham, Peribit Networks

The notion that WAN optimization is best attacked at a single layer of the Open Systems Interconnection model — Layer 5, the session layer — is intriguing. However, reality suggests otherwise. WAN performance is affected by many factors, each of which has unique characteristics that must be addressed at different OSI layers to have the greatest possible impact. Approaching the problem at too low or too high a level produces sub-optimal results.

For WAN optimization, problems should be resolved at the lowest possible layer to achieve the broadest applicability across the greatest number of applications with the least amount of complexity. Consider the two most pressing issues affecting WAN performance today: bandwidth and latency.

Solving the bandwidth problem requires reducing the amount of traffic crossing WAN links to free up additional capacity. The key to reducing WAN traffic is pattern matching — preventing redundant data from consuming valuable bandwidth by sending it once, then replacing repetitious transmissions with a tag or label.

For pattern-matching to be effective, WAN optimization products must look across multiple sessions and users to identify and remove the greatest number of repeated data patterns. While pattern-matching at Layer 5 will identify redundant patterns within a single session, it will miss repeated patterns across different sessions.

For maximum effectiveness, pattern-matching is best performed at Layer 3, the network layer, where algorithms can be applied that recognize patterns of any size, across multiple sessions and applications — including User Datagram Protocol (UDP)-based applications such as VoIP. By optimizing at a lower, protocol-independent layer, pattern matching has the greatest possible impact across the widest range of WAN traffic while being completely transparent to existing network devices and servers.

When it comes to latency, there are two issues to address, both of which require different approaches at different OSI layers. First, latency affects the performance of TCP-based applications at Layer 4, the transport layer. Because TCP restricts the amount of data sent across the WAN, traditional approaches aren't always sufficient to improve performance. The ideal solution must seamlessly replace TCP at Layer 4 with a more efficient protocol designed specifically to deal with latency and accelerate TCP-based applications.

WAN latency impacts "chatty" applications, which require hundreds or even thousands of time-consuming round trips between the client and server to complete a transmission. These applications require protocol-specific acceleration to minimize chattiness and speed up performance across the WAN. This is best addressed at the top of the OSI stack — Layer 7, the application layer. Clearly, no single OSI layer offers a magic tonic for WAN optimization. An approach that provides broad coverage with the least amount of overlap is a much better strategy.

Graham is president and CEO of Peribit, a vendor of WAN application performance products. He can be reached at jgraham@peribit.com.

More online!

Log on to Network World Fusion to voice your opinion. Face-off authors Jef Graham and Andrew Foss will add their thoughts to the discussion.

DocFinder: 6328

opinions!

ON TECHNOLOGY

John Dix

Keep this survey for future use

Companies upgrade their Ethernet switching infrastructure every four years because, in descending order of priority, the gear is near the end of its useful life, bandwidth is running out or they require new features.

Those are some of the conclusions found in a Goldman Sachs bulletin released this month that is based on a survey of 100 network managers in Fortune 1000 companies.

Unlike PCs, where purchasing cycles are more obvious because of processor advances, it has been hard to gauge LAN upgrade cycles. Goldman Sachs says its survey "showed evidence that enterprise switching equipment has a rolling upgrade cycle centered on a four-year equipment life."

And most of the companies surveyed, 46%, said end-of-life replacement is what drives their Ethernet upgrade decisions. Another 28% said they trade up because they need more bandwidth for things such as VoIP and multimedia and collaboration applications.

A smaller percentage, 19%, said they are driven to upgrade by the need for new features. More than half of the users in this camp say they are upgrading to enhance security. Of the others looking for new features, 19% cited VoIP as the driver, another 19% said they wanted to add support for wireless LANs, and 10% said they needed Power over Ethernet.

The survey also drilled down into enterprise VoIP plans. Only 29% of respondents who said they are deploying VoIP are doing so across their organizations, while the rest are implementing it in certain locations (23%) or in limited pilot groups (28%).

"The survey indicates that enterprise VoIP deployment in 2005 has momentum, but a significant portion of the 2005 deployments may be tactical rather than strategic," Goldman Sachs concludes.

For those ready to make the VoIP plunge, the survey shows Cisco is the partner of choice. Of the respondents who said they are planning to deploy VoIP equipment in 2005, 43% have Nortel PBXs today, and 38% have Avaya gear. The VoIP equipment they are most likely to migrate to? Cisco got 58% of the votes, 17% said they will use Avaya, and 13% will install Nortel.

Goldman Sachs inquired about interest in IP Centrex and found that more than a quarter of the respondents "will use VoIP services in some locations, our own equipment in others."

While the findings about upgrade cycles essentially verify what most people could have guessed, having a reputable third party put it in writing might prove useful in future project justifications.

— John Dix
Editor in chief
jdix@nww.com

Sarbox's precedents

Regarding Johna Till Johnson's column, "Hate Sarbox? Blame Bernie Ebbers" (www.nwfusion.com, DocFinder: 6327): The blame goes a lot further back. In his book *Take On the Street*, Arthur Levitt, who was chairman of the Securities and Exchange Commission in the 1990s, writes that the SEC knew there were loopholes in the law and wanted to close them, but corporations, accounting firms and investment bankers lobbied Congress to stop them. Also, remember when President George W. Bush said the accounting scandals were only the result of "a few bad apples"? Then when the WorldCom bankruptcy happened, he suddenly changed course and approved Sarbox.

If the politicians had been doing what they were supposed to, then accounting laws would have been tightened up in the 1990s instead of going way overboard when the public finally forced changes.

Les Brunswick
DeKalb, Ill.

Everything for nothing

Regarding "Shake-up in telecom has users on edge" (DocFinder: 6329): I have been in the telecom industry for more than 35 years. I was on the access/carrier side for 29 years and on the customer side for six.

It seems that corporations want everything for nothing. The push to drive down telecom prices has led to cutthroat behavior, poor business practices and situations like WorldCom. Whenever I hear managers say they want lower prices, I want to say, "The telcos have to make a profit to stay in business and deliver world-class products and services!"

Competition is good, but everyone has lost their senses in the greed for cost savings and winning business no matter the consequences. Perhaps buyers will realize they can't just count on cutting costs by driving their suppliers to the brink of disaster. Granted, there has been poor management on the telco side and poor decisions made in an attempt to be "everything" to the greedy buyer. Let's hope for a win-win environment.

Sandra Mikesell
Dayton, Ohio

E-mail letters to jdix@nww.com or send them to John Dix, editor in chief, Network World, 118 Turnpike Road, Southborough, MA 01772. Please include phone number and address for verification.

MCI is responsible

In his column "AT&T: What went wrong?" (DocFinder: 6330), Thomas Nolle doesn't mention that AT&T was forced into making the decision to spin off AT&T Broadband because Bernie Ebbers and MCI lied. If MCI hadn't fudged its numbers, Wall Street would not have hammered AT&T's stock or projected that it couldn't generate enough cash to sustain AT&T Broadband. AT&T Broadband's sell-off didn't just suddenly happen because of a bad decision to "focus on AT&T's core business" — it happened because of the fraud committed by WorldCom. I think it's important to make clear that WorldCom is largely responsible for the shambles the entire telecom industry is in, as well as for AT&T's state today.

Mahadeva Mani
Herndon, Va.

Nolle replies: WorldCom's behavior had a wide impact on the industry, but I can't assign it the blame on this one. I don't think AT&T's stock was hammered in comparison with MCI's; it was hammered because the numbers weren't there. Had MCI told the truth, they'd both have been hammered.

In a way, Wall Street was responsible for WorldCom. Had the Street not hyped the value of "Internet revenue" and encouraged everyone to shift costs and revenues to make it look like they had more, the early distortions of MCI's numbers might never have happened, and accounting issues were probably covering up the aftermath of this. It's a complicated industry, and honesty everywhere is the only right answer.

More online! www.nwfusion.com Find out what readers are saying about these and other topics. **DocFinder: 6327**

THROUGH CHANNELS

Ken Presti

Nortel's turnaround chief takes aim

If you've never heard of Clent Richardson before . . . you'll hear a lot more about him soon.

The speech was truly unique in that the "spin" was the apparent absence of "spin." Clent Richardson, the executive in charge of rebuilding Nortel's once powerful brand, last month stood in front of roughly 200 sales channel partners and openly acknowledged the sins of the past. Not a quick, "mistakes were made" statement followed by 30 PowerPoint slides on a new strategy, but a lengthy, deep and even heartfelt discussion about past leadership, integrity, transparency and a lost focus on the customer.

The partners, who earlier had listened passively, occasionally playing with their PDAs, now sat bolt upright in rapt attention. This was much closer to the core than anyone had expected. By the end of the speech, the room had a sense of common cause usually found at 12-step programs.

"I thought we were going to hear a lot more excuses," said one value-added reseller. "But that speech got my attention. Maybe they're really serious this time."

If you've never heard of Clent Richardson before — and yes, I spelled his name correctly — you'll hear a lot more about him soon. Billed as a turnaround expert previously at Apple and T-Mobile, Richardson was named Nortel's chief marketing officer last September, inheriting the uphill task of rebuilding the beleaguered company's brand strength. In his speech, Richardson addressed Nortel's woes head-on and with occasional wit.

"By being candid, you let people know that you acknowledge the problems, know what you've got to do and intend to go do it," Richardson explained in a later interview. "It wasn't risky at all. I think it's just hot air when people try to explain away what they did."

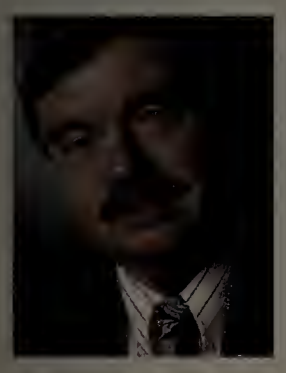
Much of the actual turnaround strategy is about reaching out to end users and building demand for the company's voice and data products. With additional customers in the fold, more channel partners would help meet the demand and make a few dollars along the way. But Nortel has a lot of ground to cover — and a lot of decisions to make — before any such success can be measured.

One key component to any effective turnaround strategy is to make tough decisions and "not get overwhelmed with consensus," Richardson explained. "We need to live by the sword and die by the sword, and I'm OK with that. I can't allow it to stop me from making decisions. We've seen a lot of that problem in corporate America. How many leaders really make a decision, as opposed to collecting consensus and looking for agreement?"

An expanded management team is now in place to help with those decisions. Nortel recently named Gary Daichendt, a former Cisco executive, as president and COO, reporting to CEO Bill Owens. The new management team plans to build a more marketing-driven company.

Whether Nortel will be able to return to its previous market stature remains to be seen. But either way, look for bold moves reflecting the intent to live or die by the sword.

Presti is research director of IDC's Network Channels and Alliances service. He can be reached at kpresti@idc.com.



REALITY CHECK

Thomas Nolle

What else don't we know about VoIP?

So here we are, with a critical program for priority communications at risk. Why did this happen?

Last month, the FCC hosted a "summit" on a topic that touches everyone yet is almost unrecognized: the Telecommunications Service Priority program. The TSP is the communications heart of U.S. plans for emergency preparedness, mandated by law and implemented on the public switched telephone network ... and we don't know for sure that VoIP can support it. Which begs the question, "What else don't we know about VoIP?"

In late 2003, the government issued a request for information (RFI) to explore the impact of IP convergence on TSP. It had two primary issues to consider. First, are there new forms of communications, enabled via IP and adopted widely by industry and the government, which must now be considered for priority treatment? Second, will TSP's treatment of voice calls and leased services work in converged networks?

The answer to the first question seems to be yes. E-mail, instant messaging and online collaboration are tools at least as valuable as voice services and thus should be included in any priority program. The problem is that there are thousands of e-mail systems and dozens of IM and collaboration systems. There is one PSTN. It was possible to create a unified TSP plan for the single PSTN, but how practical would it be to even attempt that for the plethora of new-age IP communications options?

The RFI's requirements seem to answer the second question. They talk about security, non-traceability, restorability and other things that the Internet has not been successful in providing.

In the PSTN, services are in/of the network. In IP, they're over the network. The PSTN acts as a kind of harmonizer of technology and policy, a place where common membership mandates common standards, and public policy can be applied because there's a defined and small group of companies to apply it to. The IP world lets anyone create services, which increases flexibility, but reduces the network's ability to create harmony at the service level and multiplies the number of different and possibly incompatible solutions.

I've read the TSP documents and talked with some of the people involved. In my view, voice over the Internet could not meet TSP requirements, nor could current e-mail and IM systems. Internet VPNs couldn't conform to the priority reconnection goals of the program. Not all "private IP" implementations of VoIP (where the VoIP network is partitioned from the Internet) would be much better than the vanilla Internet at complying with TSP policies. So here we are, with a critical program for priority communications at risk. Why did this happen?

First, regulations today are very PSTN-centric because we haven't had any new legislation to cover data networks and services. Even the 1996 Telecom Act didn't do data. The FCC today is trying to meet public policy goals with laws that don't reflect the new technology of IP.

Second, the standards process isn't cooperating. The IETF has regularly declined to address public policy issues in standards, including Session Initiation Protocol voice. Part of this is IETF politics, but part is also the fact that the IETF wants an absolute separation of services and networks, which makes it hard to build something as unified as the PSTN using IP.

Third, carriers aren't disclosing their "non-Internet-IP" plans or the technology on which they're based. Everything we know about VoIP comes from over-the-Internet players that don't control infrastructure and therefore can't meet TSP goals.

Finally, equipment vendors aren't bringing TSP issues to the fore, so it's not clear how or if they can support this sort of program.

TSP is a U.S. program, but there is a TSP-like requirement in nearly every major industrial country. There are many public policy goals that converged networks may not be meeting. It's disquieting that we've gotten this far in the convergence debate without exposing all the implications and issues. There are probably others yet to be exposed, and we're running out of time to deal with them.

Nolle is president of CIMI, a technology assessment firm in Voorhees, N.J. He can be reached at (856) 753-0004 or tnolle@cimicorp.com.

Real-time collaboration using presence-based tools is still a few years away for most companies.

PRESENCE SIMMERS ON BACK BURNER

■ BY MELANIE TUREK

By themselves, today's collaboration technologies, such as instant messaging and audio, video and Web conferencing, help make workers more productive. But when combined with presence — information about where users are, what applications or devices they're using and how to best reach them — those collaboration tools can become part of a virtual workplace in which employees can quickly get information they need and ad hoc groups can set up meetings on the fly.

The result: Companies save money, boost productivity and stay agile in a changing world.

It's a great goal, but it's still at least three to five years away for most organizations. That's one key finding in a recent Nemertes Research survey. Only 16% of the 43 IT executives who responded said they use presence now, another 26% plan to do so in the next six to 24 months, but that leaves 42% with no presence plans at all.

There are two main reasons why companies are holding back. Many IT executives don't see the justification, in resource terms, for deploying presence; and those that do still are focused on other real-time communications deployments, such as IM and Web conferencing.

That is expected to change over time, but until companies get a handle on IM, conferencing and basic security issues, presence will remain on the back burner for most IT executives.

Office politics

In the meantime, a war is brewing as vendors come at presence from a variety of angles. Applications vendors such as Microsoft and IBM Lotus view voice as an add-on to their collaboration products, while IP telephony vendors such as Nortel and Siemens see collaboration applications as an add-on to their voice systems.

Microsoft's Live Communications Server (LCS) 2005 is designed to work with public IM services from AOL and Yahoo, and Microsoft's own MSN Messenger. LCS 2005 also enables the integration of IM and presence awareness in other Microsoft applications, notably Office.

An MSN Messenger user will be able to IM an AOL user from within the LCS client using Session Initiation Protocol (SIP). However, a user won't be able to IM that AOL user from within an Office application, at least not yet.

Although many survey respondents purchased licenses to LCS and the IM client (often as part of a larger enterprise license agreement), most have yet to deploy it.

Those who have installed LCS still are figuring out the right strategy for the future. "We use LCS for now, we have presence in our Office applications," says Alvin Lim, general manager of the Regional Microsoft practice at Asia Datacraft. "It's not yet embedded in back-end systems. It's a great technology, but we're trying to figure out the apps that apply."

Nevertheless, survey results show that Microsoft has the largest user base among participants: 20% of companies that have standardized on an enterprise IM system use Microsoft as their vendor, and 79% say they use or plan to use LCS for embedded presence.

IBM's newest entry in the real-time communications arena is Lotus Workplace Team Collaboration, which is Java 2 Platform Enterprise Edition-based and offers integrated synchronous and asynchronous collaboration, which includes IM, presence awareness, Web conferencing, team spaces and development tools for embedding presence in enterprise applications.

Lotus is developing a SIP infrastructure for reuse across IBM software products. IBM also has defined an interdomain specification for SIP for Instant Messaging and Presence Leveraging Extensions that enables interoperability among SIP-based IM offerings. But IBM today doesn't offer interoperability with other presence and IM vendors or services.

Just 11% of companies that participated in the survey use Lotus for IM, and only 7% who've embedded presence in other enterprise applications use Lotus to do so.

Presence at work

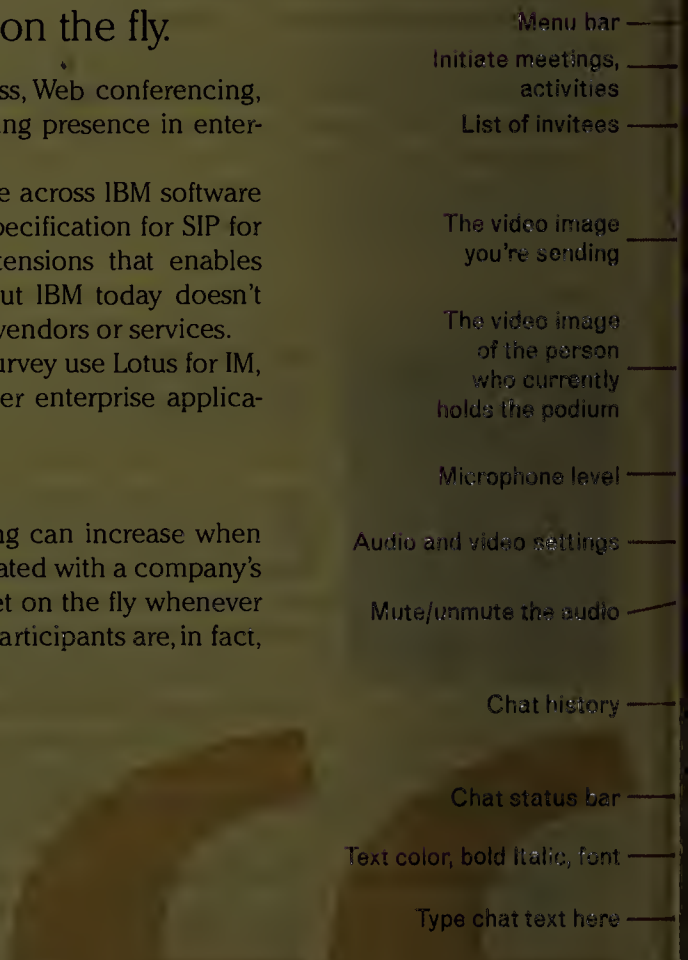
The value of audio, video and Web conferencing can increase when these services are presence-enabled and/or integrated with a company's IM system. Click-to-meet capabilities let users meet on the fly whenever and wherever they need to. Presence ensures all participants are, in fact, available for the meeting.

Some conferencing products let hosts schedule meetings to start as soon as participants are available, tapping into their online presence, their phone presence and their calendar presence. This can replace hours of coordination time and ensure meetings get done as soon as possible, which saves project time, as well.

"We love being able to jump from IM to audio or Web conferencing. We find that that's a very interesting phenomenon. Multi-party chats can escalate to voice conferencing, and they tend to do that. We're connected via the IP network, so there's no cost," Lim adds.

Convoq's ASAP is essentially a presence-enabled Web conferencing tool built on Macromedia's Flash technology. The eDial Instant Collaboration System provides enterprise-grade, secure IM, enhanced with presence, calling, and audio and Web conferencing from a user's standard Internet browser.

Meanwhile, many enterprise IM vendors are positioning themselves as presence vendors. Bantu, an enterprise IM product, integrates with WebEx Communications and Microsoft's Office Live Meeting, so users can launch a conference from within a Bantu instant message. They also can call someone simply by clicking on an audio link — and in both

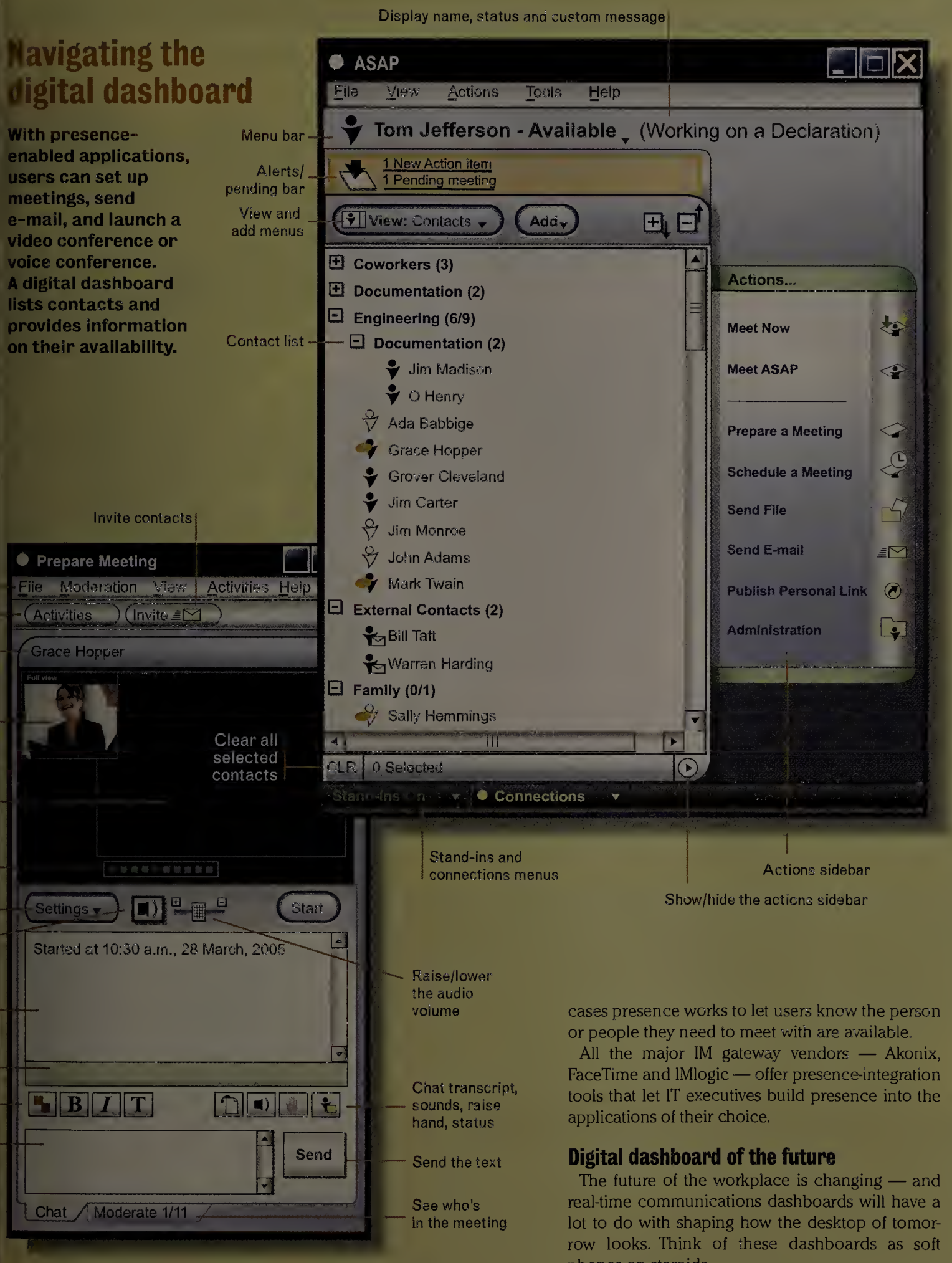


We love being able to jump from IM to audio or Web conferencing. We find that that's a very interesting phenomenon. Multi-party chats can escalate to voice conferencing, and they tend to do that. We're connected via the IP network, so there's no cost."

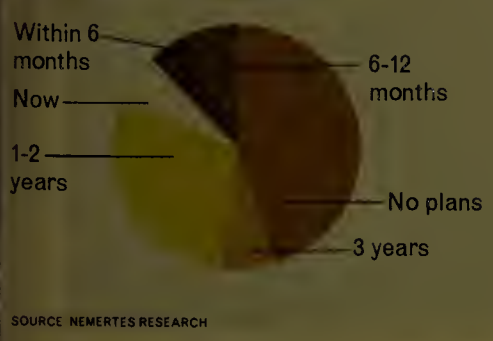
ALVIN LIM, general manager, Regional Microsoft practice, at Asia Datacraft

Navigating the digital dashboard

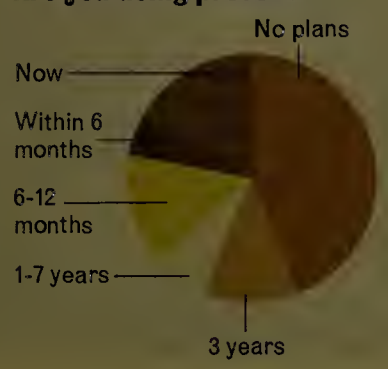
With presence-enabled applications, users can set up meetings, send e-mail, and launch a video conference or voice conference. A digital dashboard lists contacts and provides information on their availability.



Do you use or plan to use real-time communications dashboards?



Are you using presence?



SOURCE NEMERTES RESEARCH

cases presence works to let users know the person or people they need to meet with are available.

All the major IM gateway vendors — Akonix, FaceTime and IMlogic — offer presence-integration tools that let IT executives build presence into the applications of their choice.

Digital dashboard of the future

The future of the workplace is changing — and real-time communications dashboards will have a lot to do with shaping how the desktop of tomorrow looks. Think of these dashboards as soft phones on steroids.

Some traditional networking vendors, including Avaya, Nortel and Siemens, developed software designed to use IP networks and offer presence, conferencing, and integrated voice and data for total communications convergence.

Only 7% of companies report using real-time communications dashboards today. But another 40% plan to do so in the next two years. And vendors are stepping up to offer products:

- The 3Com Convergence Applications Suite incorporates the 3Com IP Messaging module for unified messaging functionality such as "read-me e-mail" and "find-me/follow-me" services; the 3Com IP Conferencing module for audio conferencing, video conferencing, data conferencing and presence management services; and 3Com's IP telephony products.
- Avaya's Converged Communications Server works with the vendor's IP telephony software, Communication Manager; supports presence; and integrates IM and telephony via a single buddy list; users can click to launch a call from within IM.

Avaya supports six-way meet-me conferencing, and it recently acquired Spectel for audio conferencing (the next release will support click-to-conferencing capabilities). The company's video conferencing telephony desktop solution integrates the vendor's soft phone with the Polycom desktop solution.

- Nortel's Multimedia Communication Server 5100 drives VoIP networks, and delivers multimedia and collaborative applications to the enterprise on an open platform that supports industry-standard protocols, including SIP and H.323. Capabilities include mobility, collaboration, presence, messaging and video services.

Collaborative applications include videoconferencing, audio and video streaming, white-boarding, file exchange and IM. Telephony services include call redirect and call forwarding, conferencing, call hold and waiting, multiple server registration, and real-time call management.

- Siemens' OpenScape lets workers see their colleagues' availability across an IP network and lets users prioritize and control who can reach them, where, and when. One-click access to WebEx Web conferencing makes it easy for people to jump into a meeting as soon as they're all available. OpenScape operates on Windows Server 2003 and enhances Microsoft e-mail and Windows Messenger, and voice and wireless communications. But its open nature lets it integrate with other enterprise applications.

Contact centers lead the way

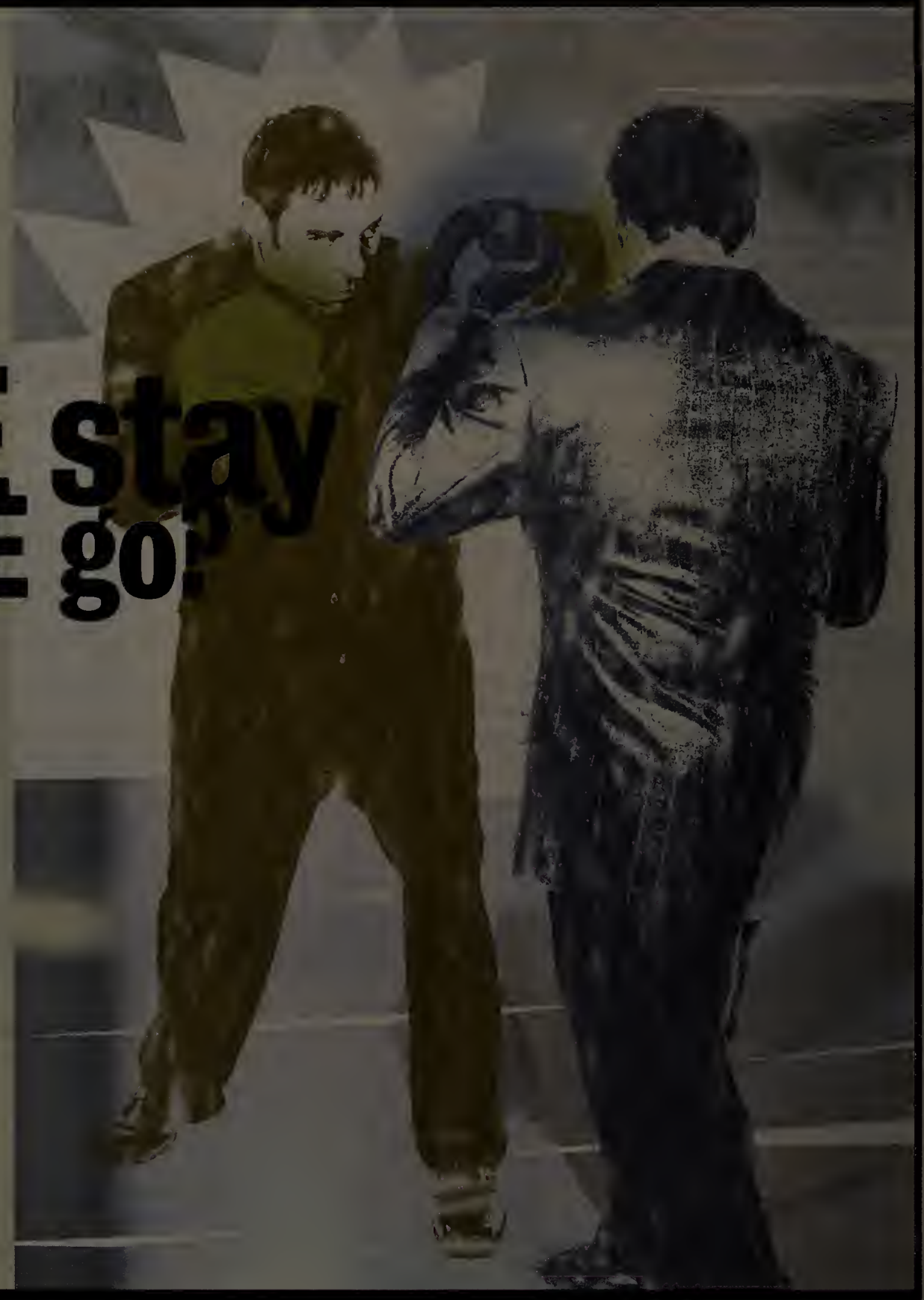
One area leading the way in the use of real-time applications is in the contact center. This is happening primarily on three fronts: Web chat between agents and customers; IM use among agents and experts to quickly distribute information and answer questions; and expert routing, which sends calls to the most appropriate available agent.

Presence has the potential to change the way people work — and how they communicate and collaborate with one another. Change will come slowly; the technology isn't as mature as it needs to be. The productivity gains are difficult to measure, and the cultural adjustments won't come easily from end users, but companies that adopt the new tools will be well positioned to support a dispersed workforce and leverage the benefits such an environment brings.

Turek is a principal research analyst at Nemertes Research. She can be reached at melanie@nemertes.com.

Microsoft's dominant browser is being challenged by open source upstart Mozilla Firefox, but in our testing neither browser scores a knockout punch.

Should IE stay or should IE go?



■ BY RODNEY THAYER, NETWORK WORLD LAB ALLIANCE

Don't go ripping out Microsoft's Internet Explorer just yet.

It certainly has proven vulnerable to attack in the past, and the constant patching to add the latest security updates can be a nuisance. CERT last year even warned people to stop using Internet Explorer. And Mozilla Foundation's Firefox has been getting a lot of buzz lately — to the tune of 25 million downloads in less than 100 days on the market.

But our testing of both browsers shows that it's not an easy decision — particularly in an enterprise environment. Internet Explorer's vulnerability to attack might in part be because it's rich in features and thereby presents a larger "attack surface." On the other hand, Firefox's perceived edge in security comes with a price — fewer features and possible inability to access some Windows-based Web applications.

So before you make a decision, weigh the trade-offs. One compromise to consider is using Internet Explorer internally and Firefox for pure Web browsing.

Our hands-on test focused on security rather than ease of use. Our Internet Explorer 6.0 implementation ran on a Windows XP client (a

See Browser, page 78

Attack profiles: Browsers go head-to-head in common attack scenarios

Attacks against browsers generally fall into three categories. **ROUND 1:** Protocol attacks against content processed directly by the browser. **ROUND 2:** Attacks against active scripting language running within the browser environment. **ROUND 3:** Attacks against data delivered through the browser but processed by a plug-in or other component such as a Dynamic Link Library that provides graphic display services.

Round 1: Slight advantage: Internet Explorer.

Internet Explorer and Firefox are both potentially vulnerable to attacks via Web site content they process directly. Internet Explorer is less vulnerable in this area probably because Microsoft has put so much work into securing its browser in response to all of the hacker activity targeting it. But theoretically, because they both process essentially the same HTML datastream format, either browser could be attacked in that manner.

Round 2: Advantage: Firefox.

In the second category, Internet Explorer provides ActiveX, JavaScript and many other mechanisms to execute code delivered through Web pages such as Visual Basic scripts or Active Server Page and .Net content. Because there are more ways to write programs that are delivered through the browser, Explorer is more susceptible to attacks in this manner. This is the downside of all those sophisticated features that work in a pure Microsoft Web environment.

Round 3: No advantage.

Both browsers support plug-ins, which, independently of the browser, can be vulnerable to attack. A recent example is the RealOne plug-in vulnerability (www.nwfusion.com, DocFinder: 6526). While this vulnerability was specifically found with Explorer, the problem lies in the plug-in and there is no technical reason to assume this sort of problem will not happen someday with Firefox.

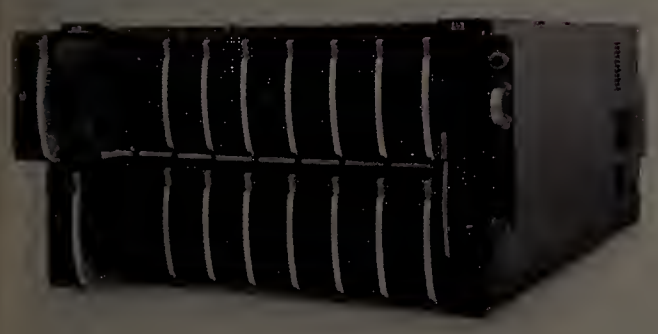
intel inside
XEON

When everything works together, everything changes together.

HP BladeSystem servers allow you to integrate your systems with ease for unexpected growth and unforeseen business demands. Powered by Intel® Xeon™ Processors, these innovative servers adapt to change in a seamless modular fashion, creating new operational efficiencies to dramatically upgrade your enterprise. And that changes, well, everything.

change

hp



HP ProLiant BL30p server blades

To read IDC's *Adapting to Change: Blade Systems Move into the Mainstream*, visit hp.com/go/bladesmag19

Solutions for the adaptive

hp

invent

Browser
continued from page 76

WinBook Pentium 4 with 512M bytes of RAM) with Service Pack 2, and the latest Microsoft updates. With the help of VMware Workstation, we installed Mozilla Firefox 1.0.1 on the same system inside its own virtual machine. This test machine was connected to the Internet through a 384K bit/sec DSL line.

We used the browsers side by side for a variety of tasks such as reading public Web sites, checking e-mail with Microsoft Outlook Web Access, and accessing our Apache-based Web server to reach internal resources and management tools. Additionally, we tried surfing to known hacker Web sites to see how the browsers would behave when under attack.

Accessing conventional Web sites, such as CNN or Yahoo, gave similar results. They both block pop-ups and offer a variety of plug-ins to support additional forms of data such as Macromedia Flash or Adobe PDF files.

However, the key difference is that because Internet Explorer contains Windows-related features that are not available in Firefox — Active X, .Net, Active Server Pages — it is difficult, if not impossible, to use some Web-based applications with Firefox.

Both Internet Explorer and Firefox have facilities to digitally sign plug-ins. However, the signature feature is not ubiquitously used, and users are quite likely to accept and execute unsigned and potentially dangerous code.

This is why you should back up your browser with an intrusion-prevention system or adequate anti-virus (ours was running F-Secure's Anti-Virus Client Security), that can detect, notify and/or block malicious code that arrives through the browser.

Rendering architectural conclusions

So does Firefox's architecture make it fundamentally more secure? What we found is that Firefox is not necessarily a more secure implementation of a browser. It simply has fewer features to attack.

It supports fewer and less complex scripting mechanisms so it is not as easy to write powerful, dangerous code inside a Web page that can attack it.

It is not as tightly integrated with any particular operating system. This means there are fewer ways the browser uses operating system-specific features. That means there is less of a chance for an exploit to use the browser as an interface into the underlying operating system.

Also, the open source nature of the code sometimes, but not in a guaranteed manner, provides more peer review of the code and faster turnaround for fixes to vulnerabilities.

The enterprise game plan

It's not realistic to think that you can totally stop using Internet Explorer, especially if your users must access servers that use the rich features it supports over an internal network or through the public Internet.

Can you start selectively using Firefox? If you have a purely browser-based environment, with standards-based scripting and plug-ins, then you can consider this.

Will it make your environment perfectly secure against browser-based attacks? No. Firefox — like other browser alternatives — is not perfect, but the attack surface can be reduced significantly if you use fewer complex features, such as sites that deliver ActiveX through Web pages.

If your network comprises thousands of users, then this can be a difficult change to execute. On the other hand, it makes sense to compare the cost of securing Internet Explorer with add-on client security products or intrusion-prevention devices to the cost of simplifying/standardizing your browser-based infrastructure.

What to do?

The risk of a browser-based attack against an enterprise network is significant. From a risk management point of view, it is definitely a good idea to look at browser alternatives to Internet Explorer purely based on the sheer number of clients running it. But the environment might not let you remove it because your shop might have built up access to necessary internal resources using Microsoft's technology based on Internet Explorer.

One possible solution would be to mandate the use of Firefox for external access and reserve Internet Explorer for inside-the-enterprise use. Policy-enforcement tools can help implement this sort of a mandate.

Security measures external to the browser, such as application firewalls, intrusion-detection and prevention systems, and the use of policy enforcement systems to ensure clients only access trusted Web sites, can also be considered to address the browser risk.

Thayer is a private network security consultant in Mountain View, Calif. He can be reached at rodney@canola-jones.com.

NetResults

Microsoft Internet Explorer

PRICE: Ships as part of Windows.

PROS:

- Complex scripting allows sophisticated delivery of services over the Web.
- Commercial browser implementation available with support and maintenance.
- Integrates well with Microsoft and other vendors' browser/Web server-based offerings.
- Continued enhancements to security, recently examples being delivery of XP Service Pack 2 and announcement of Internet Explorer 7.
- Encryption and authentication facilities available to strongly control browser access to data.

CONS:

- Complex scripting provides remote access to poorly defended system interfaces that were never designed for other than local and/or strongly authenticated use.
- In some cases, known vulnerabilities are not corrected for some time and thus exploits exist in the wild for which there is no browser update. An example is the XP SP2 pop-up problem (go to www.nwfusion.com, DocFinder: 6325, for details), which was announced in December, 2004 and which still exists in Internet Explorer 6 on XP SP2 as of early this month.

Firefox, Mozilla Foundation

PRICE: Free.

PROS:

- Standards-based browser doesn't use proprietary features.
- Popular open source project is well supported by an active community, which in some cases facilitates faster repairs.
- Source code available for review.
- More encryption features (certificate support for Online Certificate Status Protocol, more recent SSL/TLS cipher suites).
- Simpler implementation means less attack surface and fewer paths into lightly defended local system interfaces.

CONS:

- No commercial support available.

Less compatibility with proprietary, but de facto, standard Web features such as ActiveX. No guarantee of open source development team will address new vulnerabilities any faster than a commercial implementation.

New releases are coming up

Both Microsoft and Mozilla are actively working to make their browsers more secure. Internet Explorer was updated with XP SP2 to provide better checking on data delivered to plug-ins (MIME type vs. file-extension checking) and to provide more capabilities to digitally sign active scripts that are delivered to the browser. Microsoft has also moved up plans for Internet Explorer 7.0 to later this year.

Mozilla also has issued a point release of Firefox and has plans for another revision next month. Both browsers support the use of encrypted connections over SSL/TLS and authenticated Web sites. With this feature, you can control which sites users can access in an authenticated manner through digital certificates at the server and username/passwords, certificates or hardware tokens at the client.

— Rodney Thayer

Wireless nets: Leave no disaster-recovery stone unturned

■ BY JOANIE WEXLER

I've been discussing the use of wireless network services for disaster-recovery applications. While redundant buried cables strung out of the same entrance to your building can be cut at the same time with devastating results, a backhoe or other natural enemy to terrestrial cabling has no impact on airborne packets.

However, if you're really serious about high availability, you should do your homework about the design of your carrier's wireless network — just as you would with a wired infrastructure, advises Matthew Liotine, vice president at BLR Research, a technology management consulting firm.

Liotine notes that while a cable cut in the last-mile link to your premises won't affect your wireless access network, the same isn't true about shared fiber connections further down the line — say, between wireless base stations in your mobile operator's network.

True, wireless is emerging for these connections too: one of the most popular would-be applications for early WiMAX technology, for example, is for backhaul between base stations or carrier points of presence.

However, if you don't know how the carrier network is architected, you might think you're secure when vulnerabilities could be close to your doorstep. It's worth investigating to find the weak spots, Liotine says.

"The point is to seek out single points of failure and common, shared infrastructure, regardless of what type of service you are using," Liotine says.

He says if a carrier's cell site sits on a tower shared with many others, and a storm hits, "lots of [wireless] service can be wiped out."

Also, consider whether your service is offered in an unlicensed or licensed frequency. Most early WiMAX services in the U.S. will be in the 5.8-GHz unlicensed band; ask your service provider about potential interference issues, he says. If the service is in a licensed band, is it still a shared service? If so, is bandwidth guaranteed to be available to you?

"If you have a critical service, such as a daily download of business receipts, you want a dedicated [wireless] circuit," he says.

Also, be cautious of the bandwidth claims advertised by service providers. "You can't go by the typical average throughput claimed by the carriers" in terms of backup bandwidth available, Liotine says. "You must consider other factors such as wireless frequency, distance and modulation scheme. Certain modulation schemes can pump more bits per unit of frequency, which can gain you some bandwidth."

Companies should evaluate their wireless provider's core network for internal redundancies and make sure the provider shares no common infrastructure with wireline providers.

Wexler is an independent networking technology writer/editor in Silicon Valley. She can be reached at joanie@jwexler.com.

In your in-box

Sign up for this or any of *Network World's* many other e-mail newsletters.

www.nwfusion.com
DocFinder: 2778

Anti-spam technology failing? Well...

YOU'VE BEEN SCAMMED!

Meridius Security Gateway™

99% spam detection rate,
0% false positives,
100% virus blocking†

Call 1.866.895.6931 and get a $5000* trade-in credit

* Contact a BlueCat Networks representative for promotion details. Limited time offer. Promotion code: BCN-M105
† "Scanning for Spam", Network Computing Magazine Oct. 28, 2004

INSIDE·THE·DOMAIN™
www.bluecatnetworks.com/subscribe

BlueCat Networks
secure networks. simplified.

Call us:
1.866.895.6931

Schedule your free demo today.
Visit www.bluecatnetworks.com/meridius/nww

BlueCat Networks, the BlueCat Networks logo, Meridius Security Gateway and the Meridius logo are trademarks of BlueCat Networks, Inc.

Meridius Security Gateway

Management

Strategies

- CAREER DEVELOPMENT
- PROJECT MANAGEMENT
- BUSINESS JUSTIFICATION

Adapting to automation

Technology threatens to eliminate many of today's network administration positions, although industry watchers predict more strategic IT jobs to evolve.

CHALLENGE RESPONSE

A five-part series on how to turn challenges into opportunities.

Part 5 of 5

■ BY DENISE DUBIE

Editor's note: This is the final installment of a five-part series on the threats facing IT executives and how to mitigate them.

An old IT industry joke suggests automation will be so prevalent in future data centers that the only staff on hand will be a man and a dog: The man's job is to feed the dog, and the dog's job is to ensure the man doesn't touch the computer.

CHALLENGE

Automation technology poses a threat to many of today's IT application, infrastructure and operations positions, which could lead to the end of IT departments if remaining positions become absorbed or outsourced.

RESPONSE

By mastering automation technologies, learning best practices and incorporating business savvy into their skills, IT executives can adapt and expand beyond current operations and maintenance roles to become leading-edge technical strategists for their companies.

While the scenario of such an automated IT environment gets laughs among network executives, the premise isn't so far-fetched anymore. Today, automation technology has evolved beyond simple system monitoring to dynamic provisioning and reallocating of data center resources. New technologies such as virtualization are designed to further remove the need for human intervention from day-to-day data center operations — making the prospect of being displaced by technology no laughing matter to some.

According to Gartner, 90% of the work of IT departments surveyed last year will be automated, outsourced or absorbed by other business units by 2015. The research firm also predicts that twice as many jobs will be lost between 2005 and 2015 because of IT automation, as compared with IT outsourcing. Lastly, Gartner says it expects a typical IT department of 100 employees today to shrink to between six and 15 employees by 2015.

Time will tell if the numbers will hold true, but in the meantime, industry watchers and IT executives say when faced with such a bleak outlook for the future, one has to read between the lines. If automation is forecast to eliminate most of today's IT jobs, then the assumption should be that tomorrow's IT jobs would encompass a new set of skills yet to be tackled by technology or technicians. For instance, network operations positions would adapt into managers of strategic technology, and application maintenance roles could evolve into business services managers.

"I have been in IT for more than 30 years and I have heard about the threat of automation since Day One," says Shivaji Huttler, database and data warehouse manager for the city of Boise, Idaho. "It's really only a threat to individuals who aren't willing to adapt and evolve."

Huttler says without automation he'd be shackled to a database anxiously pouring over logs to determine if anything had gone awry. With BMC Software's Patrol automated monitoring tools in place to alert him of performance exceptions, he is free to diagnose higher-level problems and use his knowledge for business-oriented planning.

"Automation increases my productivity and empowers me with more knowledge because I am not focused on repetitive, manual tasks," Huttler says. "Databases are pretty straightforward; the exciting part is using the data toward business intelligence goals."

Huttler admits his IT operations remain far from the dynamic data centers envisioned by vendors such as HP, IBM and others, but his attitude could guarantee him a job when automation technology takes over more manual tasks.

"If you look at the big picture, automation will predominantly lead to advancement for motivated IT professionals," says Terry Phillips, branch manager at IT staffing firm Robert Half Technology in Columbus, Ohio.

Network administrator roles might be the first positions replaced by automation, but the people filling the positions could develop their skills in niche technologies such as security, wireless or network architecture to move from an operations job to a more strategic position for the time being. Positions in project management, compliance management and business process management could crop up as network administrator jobs fall off.

"There are soft skills that humans possess and technology cannot automate, especially if it's specific to one company or type of business," Phillips says. "In some cases, automation may replace a human position for the short term, but if the IT department is thinking strategically, those positions manifest themselves into something else over the long term."

Keeping valued employees familiar with the workings of the business or industry might also pay off for employers looking to automate parts of the IT department.

"You need humans to create competitive processes — you can find software that would increase the effectiveness of the process — but you need humans drafting, maintaining and updating the business processes," says Rich Ptak, a principal analyst at Ptak, Noel & Associates.

Ptak says companies looking to implement a dynamic data center that can respond automatically to changing business requirements will want to incorporate automation technology alongside strategic staff members in their deployment. "Automation will at first free up IT folks from repetitive and predictable tasks like monitoring and enable them to focus on business-oriented tasks such as rolling out new revenue-generating services," he says.

W. Kevin Colwell, development manager at Capital District Physicians' Health Plan in Albany, N.Y., says automation lets his staff work more flexibly and tackle broader tasks than in the past. With software monitoring server health and status, a systems administrator can spread his wings to explore more advanced IT duties such as provisioning new servers to support business applications.

Colwell uses Remedy software to automatically track changes and determine when human involvement is required, doing the job formerly done by two or three technicians. While automation could eliminate entry-level positions, Colwell says he doesn't believe the technology overall can be seen as a threat to the IT organization. He says automation technology — and the IT department as keepers of such — will represent a more critical role to the business going forward.

IT management often saw automation as a means to increase productivity, but Colwell says current and future IT managers will realize the technology's benefits in terms of process and business best practices. For his organization, healthcare regulations such as HIPAA forced the adoption of consistent best practices and processes.

"You need people to determine the way to approach processes in their organization; then automation helps prevent staff from straying from those processes," he says. ■

ILLUSTRATION: RON CHAN

NETWORK INSTRUMENTS

OBSERVER

How much can your network analyzer see?

Observer is the only fully distributed network analyzer built to monitor the entire network (LAN, 802.11a/b/g, Gigabit, WAN). Download your free Observer 10 evaluation today and experience more comprehensive real-time statistics, more expert events, and more in-depth analysis letting you dive deeper into your network than ever before. Choose Observer.

-DANGER- Guard against the latest network threats by identifying and isolating infected systems automatically.

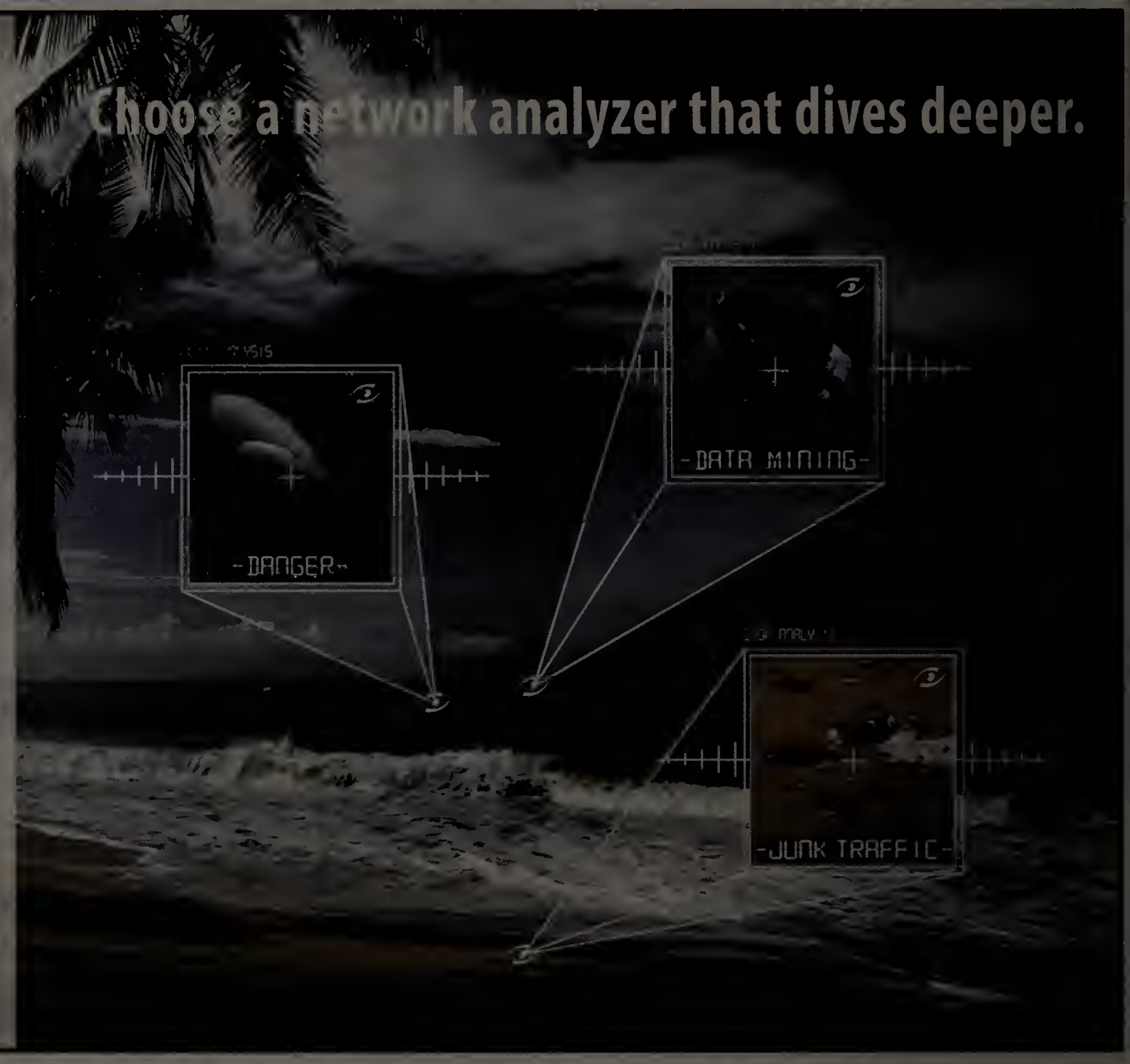
-DATA MINING- Analyze gigabit traffic and massive amounts of data with Observer's expanded options for data mining.

-JUNK TRAFFIC- Identify broadcast storms, monitor excessive traffic, and optimize bandwidth with Observer's many utilization metrics and over 30 real-time statistics.

US & Canada toll free 800.526.5958
fax 952.932.9545

UK & Europe +44 (0) 1959 569880

www.networkinstruments.com/analyze



A KVM switch allows single or multiple workstations to have local or remote access to multiple computers located in server rooms or on the desktop regardless of their platforms and operating systems. KVM switches have traditionally provided cost savings in reducing energy and equipment costs while freeing up valuable real estate.

Recognized as the pioneer of KVM switch technology, Rose Electronics offers the industry's most comprehensive range of server management products such as KVM switches, extenders and remote access solutions. Rose Electronics products are known for their quality, scalability, ease of use and innovative technology.

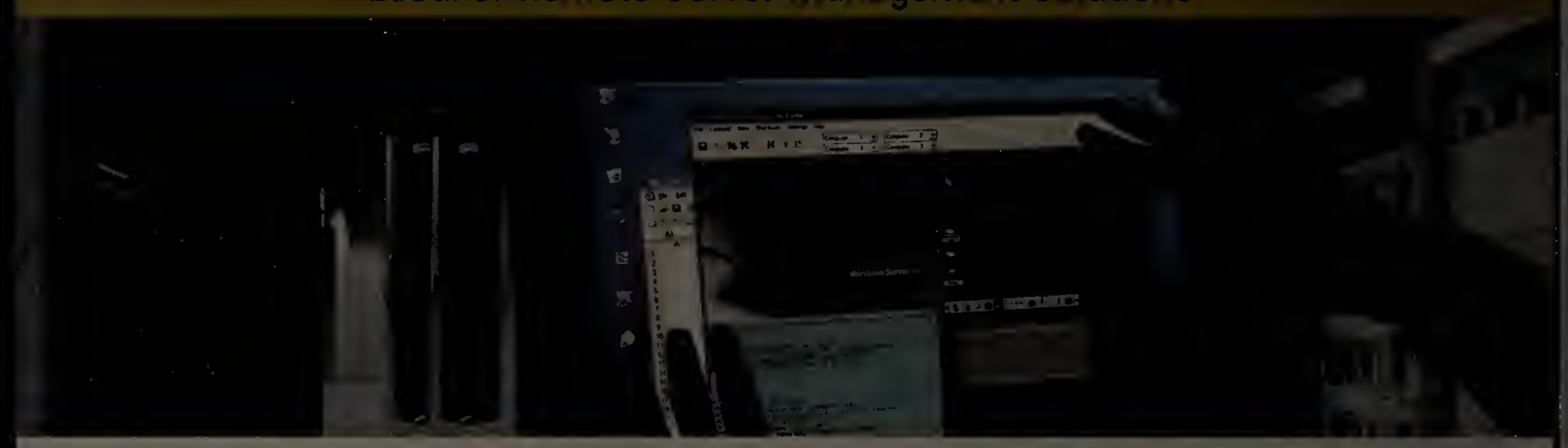
Rose Electronics is privately held with world-headquarters in Houston, Texas and sells its products worldwide through a large network of Resellers and Distributors. Rose has operations in the United Kingdom, Spain, Germany, Benelux, Singapore and Australia.

Rose Electronics
10707 Stancliff Road
Houston, Texas 77099

ROSE US +281 933 7673
ROSE EUROPE +44 (0) 1264 850574
ROSE ASIA +65 6324 2322
ROSE AUSTRALIA +617 3388 1540

SERVERS WITHIN YOUR REACH FROM ANYWHERE

Local or Remote Server Management Solutions



UltraMatrix Remote™

REMOTE MULTIPLE USER
KVM MATRIX SWITCH
ACCESS OVER IP OR LOCALLY

- Connects 1,000 computers to multiple user stations over IP or locally
- High quality video up to 1280 x 1024
- Scaling, scrolling, and auto-size features
- Secure encrypted operation with login and computer access control
- Advanced visual interface (AVI)
- No need to power down servers to install
- Free lifetime upgrade of firmware
- Available in several models
- Easy to expand

UltraConsole™

PROFESSIONAL SINGLE-USER
KVM SWITCH SUPPORTS UP
TO 1000 COMPUTERS

- Connects up to 1000 computers to a KVM station
- Models for 4, 8,16 computers
- Advanced visual interface (AVI)
- Compatible with Windows, Linux, Solaris, and other O/S
- Connects to PS/2, Sun, USB, or serial devices
- Converts RS232 serial to VGA and PS/2 keyboard
- Free lifetime upgrade of firmware
- Security features prevent unauthorized access
- Full emulation of keyboard and mouse functions for automatic, simultaneous booting
- Easy to expand

800 333 9343
WWW.ROSE.COM

ROSE ELECTRONICS

Cyclades
KVM over IP

Enjoy the magic

Secure KVM over IP switch

Web-based access

Centralized system management

Remote incident resolution

Cyclades AlterPath™ KVM/net offers a unique set of features:

- Server-based authentication
  (NT domain, LDAP, Secure ID, RADIUS, TACACS+)
- 16 and 32 port models
- CAT5 cabling up to 500 feet
- User access logging
- System event syslog
- Integrated power management

We've worked our magic.
Now you can work yours.

Over 85% of Fortune 100 choose Cyclades.

www.cyclades.com/nw

1.888.cyclades · sales@cyclades.com

cyclades

©2004 Cyclades Corporation. All rights reserved. All other trademarks and product images are property of their respective owners. Product information subject to change

The Truth about Secure-Out-Of-Band

Terminal server vendors, who proclaim that they have Secure Out Of Band products, rely on RADIUS, TACACS+ and other in-band protocols to provide security. By inference, they imply they secure out of band access when, in fact, they offer only network security, which conflicts with out of band access.

A true Secure Out of Band Management solution should provide strong security without reliance upon network-based protocols.

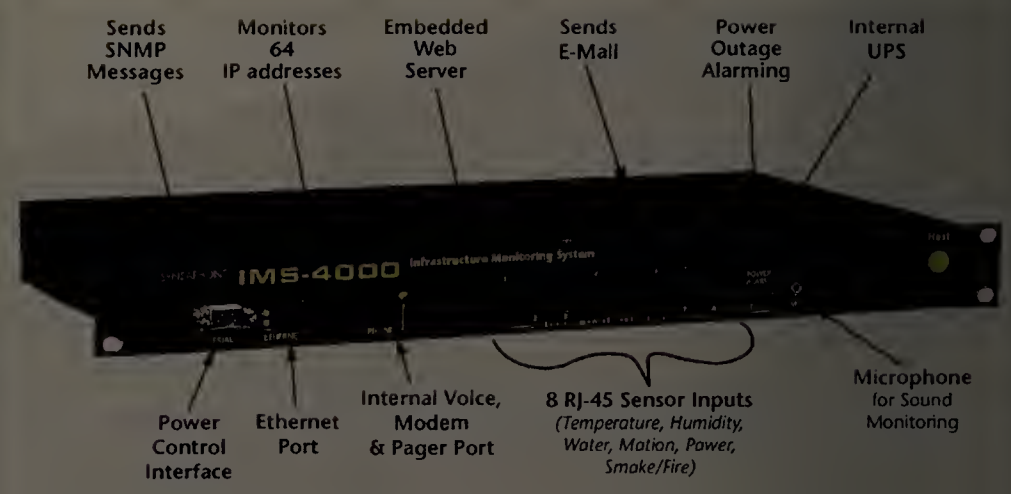
CDI offers:

- Hardware encryption over dial-up and network connections
- RSA certified SecurID authentication without a network.
- Patented central management of all remote devices
- Full NIST, FIPS 140-2 certifications
- Remote Power control
- Homologous world-wide approved internal modems

CDI has been building encryption equipment for over fifteen years. Our customers and partners include major financial institutions, government agencies, major telcos, utilities, and the United States military.

Communication Devices Inc.
www.outofbandmanagement.com

SENSAPHONE®
IMS-4000



BE NOTIFIED BEFORE CRITICAL EVENTS TURN INTO DISASTER!

- Eight environment inputs
- Power sensing
- Monitors 64 IP addresses
- Send alerts to 64 people
- 8 methods of contact
- Calendar scheduling
- Expands to 256 sensors
- Remote power control
- Optional camera

The Sensaphone IMS-4000 Infrastructure Monitoring System monitors critical environmental and network elements in your server room, data center, or telecomm installation and reports to you instantly when events threaten your infrastructure. The IMS-4000 keeps watch so you don't have to. See these features and more on the web at www.ims-4000.com

Tel: 877-373-2700
www.ims-4000.com

Phonetics, Inc.
901 Tryens Road
Aston, PA 19014

YOU WANT COMPLETE VISIBILITY.

WE MAKE IT HAPPEN.

Remote Monitoring Solutions
RMON and HCRMON Probes

You want remote monitoring solutions for visibility into every part of your network. With RMON and HCRMON Probes from Network Instruments, it's easy. Convert any PC into a complete remote network monitoring data collection device. Use the RMON appliance (available in 1U and 4U systems) for a full turn-key solution. **Call 800-526-7919** for more information or **visit our website at www.networkinstruments.com/RMON.**

- Full compliance with RMON1, RMON2 and HCRMON
- High capacity RMON Probes provide full-duplex Gigabit capture compatible with any RMON management console or collection facility (Observer®, OpenView, Concord®, NetScout®, Micromuse™)
- Complete, industry standard, software-based probes for Windows 2000/XP
- Software based, non-dedicated data collection
- Compatible with Network Instruments' optimized ErrorTrak™ NDIS drivers, which display true errors-by-station.

One Network Complete Control
Wired to Wireless • LAN to WAN

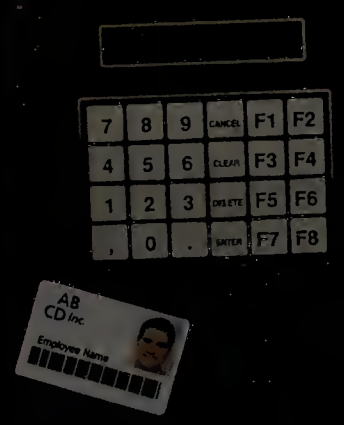
NETWORK INSTRUMENTS
US & Canada: (952) 932-9899
Toll free: (800) 526-7919
UK & Europe: +44 (0) 1959 569880

OBSERVER® OBSERVER® PROBE

www.networkinstruments.com/RMON

© 2003 Network Instruments, LLC. All rights reserved. Network Instruments, Observer, ErrorTrak and the Network Instruments logo are trademarks or registered trademarks of Network Instruments, LLC. All other trademarks, registered or unregistered, are sole property of their respective owners.

Production Tracking Over Ethernet



Eliminate your shop-floor PCs with ...

Ethernet Terminals from ComputerWise connected to your in-house LAN. Capture production data directly into files on your server.

Features & Benefits

- **Interactive Telnet Client**
- **TCP/IP over 10/100BaseT Ethernet**
- **Built-in Barcode Badge Reader**
- **Optional Mag-Stripe & RFID Badge Reader**
- **Auxiliary RS-232 Serial port**
- **Customizable Data Collection Program Included**
- **Larger keyboard and display sizes available**

COMPUTERWISE.
Call 1-800-255-3739 or visit www.computerwise.com

Aluminum Cabinets provide protection against dust, moisture, and EMI

The new Form 4 range of rugged aluminum cabinets from Optima EPS has been designed to provide reliable protection to UL-508 Type 12 specifications, as well as offering options for up to 100dB of EMI attenuation. The cabinets are easily customized to suit the required height, depth, and width, including 19" and 24" widths

The combination of Nema 12 protection and RFI shielding in a low weight cabinet makes the Form 4 cabinet suitable for a wide range of applications, such as computer simulation, test and measurement, industrial control, and computer storage installation. For maximum flexibility, the reinforced doors are field-reversible and open 122 degrees for access, with concealed hinges and multipoint locking for security and clean lines.

We deliver customized 19-inch cabinets in just 2 weeks

Every electronic system is different, so its not surprising that standard 19-inch cabinets don't always offer the ideal system packaging. That's why Optima has introduced the Custom Cabinet 14 service: customized cabinets delivered to your door in just 14 days.

You decide where you want the holes and handles. How many shelves you need. Where the doors should be. And what accessories you want. Then we put it together - fast.

So, with the Optima EPS Custom Cabinet 14 service, you don't have to keep space hungry, expensive inventory, because your ideal cabinet is just 2 weeks away.

Wall-mount swing frame suits both electrical wiring and 19" electronic equipment applications.

Optima EPS announces the launch of a versatile range of wall-mount swing frame cabinets, designed to suit both electrical wiring and electronics applications. Locks to the rugged front and rear doors permit the whole frame to clear the wall to simplify installation and maintenance for electrical contractors and manufacturing, instrumentation, and automation applications. The Frame is designed to accept standard 19" racks and fittings, as well as electrical components, and is available in a range of colors and six standard sizes from 23" x 14" to 48" x 20".

Cabinet Passes NEBS Level 4

This range of 19" and 24" wide cabinets use welded aluminum construction to provide lower weight NEBS compliance for seismic regions. Heavy-duty-aluminum extrusions are combined with seven-guage steel base to provide a rugged floor-mounting design able to resist shock, bending and vibration stresses. The cabinets are designed for deployment in earthquake-prone areas to Zone 4, and comply with Belcore TR-63/ANSI-329, suiting applications in defence, rack-mount computers, manufacturing, and telecom.

If we can do this then your server application is safe with us!

NEBS Compliant Seismic Cabinet

Optima's rugged design is the earthquake and vibration resilient foundation you need to securely protect and support your equipment. Our knowledge and design experience has enabled us to manufacture over 5000 seismic hardened cabinets which are installed in Zone 4, NEBS Compliant infrastructures worldwide!

Our vast product range and our ability to customize cabinets, consoles, and instrument cases make optima the ideal choice for all your enclosure needs.

Visit us at www.optimaeps.com to find out more or call us today on 770-496-4000

Custom
Commercial
Telecom
Seismic
EMC
Desk Systems
Instrument Cases
Accessories

Optima EPS
Cabinets & Enclosures
An ELMA Company

How Do You Securely Reboot via IP?

Sentry Gives You Secure Web/IP Based Remote Site Management

"NEW!" Secure Shell (SSHv2) Encryption «
"NEW!" SSLv3 Secure Web Browser «
"NEW!" Active Directory with LDAP «
SNMP MIB & Traps «
Integrated Secure Modem «
True RMS Power Monitoring «
Outlet Receptacle Grouping for Dual-Power Servers «
Fail-Safe Transfer Switch for Single-Power Supply Servers «
Power-up Sequencing Prevents Power In-rush Overload «
Temperature & Humidity Environmental Monitoring «
Zero U & Rack-mount Models «
110/208 VAC Models with 30-Amp Power Distribution «
NEBS Approved -48 VDC Models Available «

Server Technology

Solutions for the Data Center Equipment Cabinet

When servers and network devices in the data center lock-up, network managers need fast, secure and reliable tools to respond. With Sentry™ Remote Site Managers, an administrator can immediately reboot a remote system with just a few mouse clicks. Sentry also provides accurate input current power monitoring, environmental monitoring and integrated secure console management using SSH.

Server Technology, Inc.

Server Technology, Inc.
1040 Sandhill Drive
Reno, NV 89521
USA

toll free +1.800.835.1515
tel +1.775.284.2000
fax +1.775.284.2065
www.servertech.com
sales@servertech.com

nsai ISO 9001:2000 QUALITY

©Server Technology, Inc. Sentry is a trademark of Server Techno ogy. ©

dtSearch® Instantly Search Gigabytes of Text Across a PC, Network, Intranet or Internet

Publish Large Document Collections to the Web or to CD/DVD

- over two dozen indexed, unindexed, fielded & full-text search options
- highlights hits in HTML, XML, & PDF while displaying embedded links, formatting & images
- converts other file types (word processor, database, spreadsheet, email, ZIP, Unicode, etc.) to HTML for display with highlighted hits

"The most powerful document search tool on the market" –*Wired Magazine*

"Intuitive and austere ... a superb search tool" –*PC World*

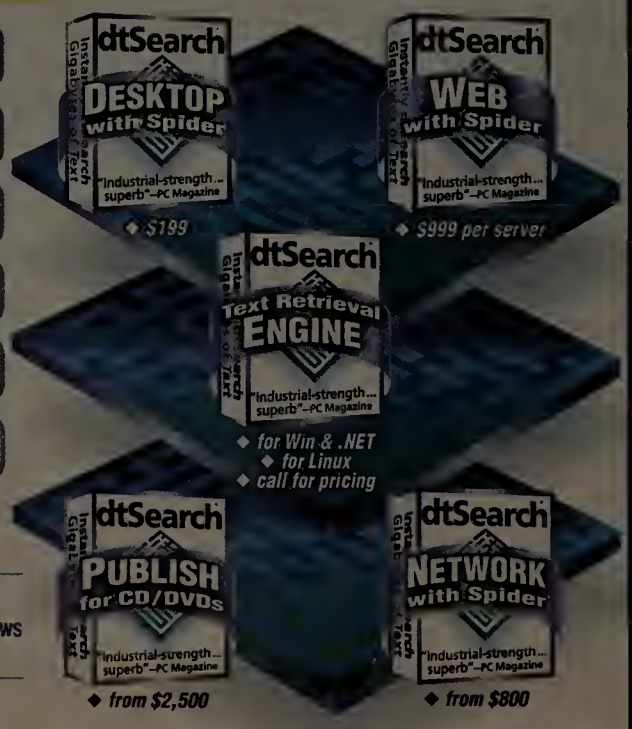
"Blindingly fast" –*Computer Forensics: Incident Response Essentials*

"A powerful arsenal of search tools" –*The New York Times*

dtSearch "covers all data sources ... powerful Web-based engines" –*eWEEK*

"Searches at blazing speeds" –*Computer Reseller News Test Center*

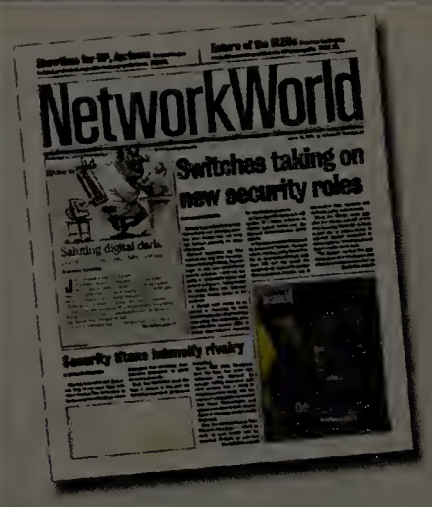
In the past two years, over half of the Fortune 15 purchased dtSearch *developer* or *network* licenses.



See www.dtsearch.com for:
- hundreds of developer case studies & reviews
- fully-functional evaluations

1-800-IT-FINDS
sales@dtsearch.com

The Smart Choice for Text Retrieval® since 1991



Reading someone else's issue of NetworkWorld®?

Subscribe today and receive your own 1-year subscription for FREE –

a $129.00 value!

Go to http://subscribenw.com/mynw for your free subscription.

WWW.SUITCASE.COM

Luggage, Fine Leather Goods, Gifts, and more!
Tumi, Hartmann, Andiamo, Samsonite, Cross
10% discount for Network World readers
Enter code NWW 2005

NetworkWorld

Editorial Index

A
Akamai Technologies 10
AT&T 10, 63
Azaleos 17

C
CipherTrust 17

E
Equant 63
Extreme Networks 20

F
Foundry Networks 20

G
GN Netcom 70
Google 6

I
IBM 19, 27

K
Kazeon Systems 88

L
LG 70

M
McAfee 17
MCI 6
Microsoft 19, 24, 27, 76
Mozilla Foundation 76

N
Netgear 67
NetPro 17
NFR Security 17
Nortel 1, 51

O
Oblix 17
Oxford Computer Group 17

P
Plantronics 70
PointBridge 17

Q
Qwest 6

R
Research In Motion 70

S
Speedera Technologies 10
Sprint 63, 70
SPSS 23
Symantec 18

U
United Devices 23

V
Vintela 17

Z
Zultys Technologies 89

Advertiser Index

Advertiser	Page #	URL
ADIC	15	www.adic.com/i2k
Barracuda Networks	9	www.barracudanetworks.com/ifor
BlueCat Networks	80	www.bluecatnetworks.com/meridius/nww
CapRock Communications	16	www.caprock.com
Communication Devices Inc	84	www.outofbandmanagement.com
Computerwise	84	www.computerwise.com
Cyclades Corp	83	www.cyclades.com/nw
dtSearch	86	www.dtsearch.com
Force10 Networks	30	www.force10networks.com
Foundry Networks	91	www.foundrynet.com/SIF
Hewlett Packard	29	www.hp.com/network/moreprocurve
Hewlett Packard	77	hp.com/go/bladesmag19
IBM Corp	11	ibm.com/eserver/pumpup
IBM Corp	92	ibm.com/db2/swap
Internet Security Systems Inc	18-19	www.iss.net/proof/wp
IT Watchdogs	86	ITWatchdogs.com
Juniper Networks Inc	13	www.juniper.net/solutions/literature/
Layton Technology Inc	79	www.auditwizard.com
Linksys	66	www.Linksys.com/SRX
MediaLive International	22	www.interop.com
Microsoft Corp	21	microsoft.com/biztalk
MRV	24	mrv.com/nww
Network Instruments LLC	82	www.networkinstruments.com/analyze
Network Instruments LLC	84	www.networkinstruments.com/RMON
Optima EPS	85	www.optimaeps.com
Oracle Corp	4	dell.com/database
Phonetics Inc	84	www.ims-4000.com
Redline Networks	2-3	www.redlinenetworks.com/infocenter
Rose Electronics	82	www.rose.com
SAS	7	www.sas.com/spent
Server Technology Inc	86	www.servertech.com
SonicWALL	25	www.sonicwall.com/csm
Websense	65	www.websense.com/patch5

New Data Center - Status Report

American Power Conversion	9	http://promo.apc.com
AT & T	32	att.com/transform
Avocent	31	www.avocent.com/control
CrossTec Corp	28	www.CrossTecCorp.com
DuPont	21	teflon.com/cablingmaterials
EMC Corp	13	www.emc.com/solutions
Fluke Networks	19	www.flukenetworks.com/APM
IBM Corp	15	ibm.com/middleware/identity
IBM Corp	16-17	ibm.com/Information
Oracle Corp	11	oracle.com/datahub
Raritan Computer	29	www.The MotherofAllAlarmStorms.com
Secure Computing Corp	25	www.securecomputing.com/goto/blackhat
Sophos Inc	27	stopthethreat.com
Sun Microsystems Inc	4	sun.com/sungrid
Sybari Software	23	www.sybari.com/nw05
Trend Micro Inc	2-3	www.trendmicro.com/cisco
VeriSign Inc	7	www.VeriSign.com

Network World Perspectives

Cisco Systems	23	cisco.com/domore

Network World Fusion - www.nwfusion.com

3Com	Network Associates
ADIC	Nokia
Airespace	Nortel Networks
Allot Communications	Oracle Corporation
Avaya	PatchLink Corporation
BMC	Program Deliverables
Broadcom Corporation	Qwest Communications
CDW	RADWARE
Ceonex, Inc.	Redline Networks
Chantry Networks	Remedy
Cisco Systems, Inc.	Riverbed Technology
Computer Associates	RSA Security Inc.
DuPont	SBC
EMC Corp	Schmidt's LOGIN GmbH
Engenio	Sprint
Finisar Corp	SSH Communications
Groundwork	Statscout Pty Ltd
HP	Texas Instruments
IBM	Trend Micro
Imprivata	TrendsMedia Inc.
Intel Corporation	Tripp Lite
IronPort Systems	VeriSign Inc
Juniper Networks Inc	Verizon Wireless Broedband
Lucent Technologies	Webroot
Meru	Xerox
Microsoft Corporation	

These indexes are provided as a reader service. Although every effort has been made to make them as complete as possible, the publisher does not assume liability for errors or omissions.

*Indicates Regional Demographic

NetworkWorld Events and Executive Forums Network World Events and Executive Forums produces educational events and executive forums worldwide, including our one day Technology Tours, customized on-site training, and executive forums such as DEMO®, DEMOmobile®, and VORTEX, as well as the DEMOletter and VORTEX Digest newsletters. For complete information on our current seminar offerings, call us at 800-643-4668 or go to www.nwfusion.com/events.

Publicize your press coverage in *Network World* by ordering reprints of your editorial mentions. Reprints make great marketing materials and are available in quantities of 500 and up. To order, contact Reprint Management Services at (717) 399-1900 x129 or E-mail: mshoben@reprintbuyer.com

Network World, Inc.

118 Turnpike Road, Southborough, MA 01772
Phone: (508) 460-3333

TO SEND E-MAIL TO NWW STAFF
firstname_lastname@nww.com

Evilee Thibeault, CEO/Publisher
John Gallant, President/Editorial Director
W. Michael Draper, Chief Operating Officer
Eleni Brisbois, Administrative Planning Manager

FINANCE
Mary Fanning, Vice President Finance
Paul Mercer, Finance Manager
Betty Amaro-White, Event Finance Manager

HUMAN RESOURCES
Eric Cormier, Sr. Human Resources Generalist

MARKETING
Terry Ann Croci, Sr. Director of Customer Experience
Nancy Sarlan, Corporate Marketing Communications Mgr.
Barbara Sullivan, Senior Research Analyst
Judy Schultz, Marketing Design Manager
Cindy Panzera, Marketing Designer

PRODUCTION SERVICES
Greg Morgan, Senior Director, Production Services
Karen Wallace, Senior Director, Advertising Operations
Mike Guerin, Manager of Production Technologies
Jami Thompson, Sr. Production Coordinator
Veronica Trotto, Online Operations Coordinator
Jane Wilbur, Online Ad Traffic Coordinator
Maro Eremyan, Advertising Coordinator
Christina Pankievich, Advertising Coordinator

CIRCULATION
Richard Priante, Senior Director of Circulation
Bobbie Cruse, Subscriptions Manager
Mary McIntire, Sr. Circulation Marketing Manager

RESEARCH
Ann MacKay, Research Director

DISTRIBUTION
Bob Wescott, Distribution Manager/(508) 879-0700

IDG LIST RENTAL SERVICES
Amy Bonner, Account Executive
P.O. Box 9151, Framingham, MA 01701-9151
Toll free: (800) 434-5478 ext. 6026/Direct:(508) 370-0826
Fax: (508) 370-0020

SEMINARS, EVENTS AND IDG EXECUTIVE FORUMS
Neal Silverman, Vice President of Events & E. F.
Mike Garity, Director of Business Development
Michele Zarella, Director of Operations
Dale Fisher, Senior Event Planner
Jacqueline DiPerna, Event Coordinator
Karen Bornsteln, Sales Operations Specialist
Danielle Bourke, Event Operations Coordinator
Andrea D'Amato, National Sales Director Events
Kristin Ballou-Cianci, Event Regional Account Director
Jennifer Sand, Regional Account Manager
Cedric Fellows, Regional Account Manager
Mark Hollister, Senior Director of Event Marketing
Debra Becker, Dir., Marketing & Audience Development
Sara Nieburg, Senior Marketing Manager
Dori Smith, Event Database Manager
Buster Paris, Marketing Specialist

ONLINE SERVICES
Kevin Normandeau, Vice President, Online
Dan Gallagher, Director of Audience Development, Online
Adam Gaffin, Executive Editor, Online
Melissa Shaw, Managing Editor, Online
Jason Meserve, Multimedia Editor
Sheryl Hodge, Sr. Online Copy Chief
Deborah Vozikis, Design Manager Online

CLIENT SERVICES
W. Michael Draper, Chief Operating Officer
Sharon Stearns, Director of Client Services
Leigh Gagin, Client Services Manager
Kristin Miles, Client Services Specialist

INFORMATION SYSTEMS/BUSINESS SERVICES
W. Michael Draper, Chief Operating Officer
Tom Kroon, Director of Systems Development
Anne Nickinello, Senior Systems Analyst
Puneet Narang, Manager of Database Technologies
William Zhang, Senior Software Engineer
Manav Seghal, Senior Software Engineer
Rocco Bortone, Director of Network IT
Peter Hebenstreit, Senior Network/Telecom Engineer
Brian Wood, Senior Systems Support Specialist
Frank Coelho, Senior Manager, Business Services
Mark Anderson, Business Services Supervisor
Linda Cavanagh, Business Services Administrator

IDG

Patrick J. McGovern, Chairman of the Board
Pat Kenealy, CEO

Network World is a publication of IDG, the world's largest publisher of computer-related information and the leading global provider of information services on information technology. IDG publishes over 275 computer publications in 75 countries. Ninety million people read one or more IDG publications each month. *Network World* contributes to the IDG News Service, offering the latest on domestic and international computer news.

Sales Offices

Cerol Lasker, Associate Publisher/Vice President
Jane Weissman, Sales Operations Maneger
Internet: clasker, jweissman@nww.com
(508) 460-3333/FAX: (508) 460-1237

New York/New Jersey
Tom Davis, Associate Publisher, Eastern Region
Elisa Della Rocco, Regional Account Director
Agata Joseph, Senior Sales Associate
Internet: tdavis, elisas, ajoseph@nww.com
(201) 634-2300/FAX: (201) 634-9286

Northeast
Elisa Della Rocco, Regional Account Director
Internet: elisas@nww.com
(508) 460-3333/FAX: (508) 460-1237

Mid-Atlantic
Jacqui DiBianca, Regional Account Director
Agata Joseph, Senior Sales Associate
Internet: jdibian, ajoseph@nww.com
(610) 971-1530/FAX: (610) 975-0837

Midwest/Central
Eric Danetz, Regional Account Director
Agata Joseph, Senior Sales Associate
Internet: edanetz, ajoseph@nww.com
(201) 634-2314/FAX: (201) 712-9786

Southeast
Don Seay, Regional Account Director
Agata Joseph, Senior Sales Associate
Internet: dseay, ajoseph@nww.com
(404) 504-6225/FAX: (404) 504-6212

Northern California/Northwest
Sandra Kupiec, Associate Publisher, Western Region
Karen Wilde, Regional Account Director
Courtney Cochrane, Regional Account Director
Vanessa Tormey, Regional Account Manager
Teri Marsh, Sales Assistant
Jennifer Hallett, Sales Assistant
Internet: skupiec, kwilde, ccochrane, vtormey, tmarsh, jhallett@nww.com
(510) 768-2800/FAX: (510) 768-2801

Southwest/Rockies
Becky Bogart Randell, Regional Account Director
Internet: brandell@nww.com
(949) 250-3006/FAX: (949) 833-2857

Online/Integrated Solutions
Kevin Normandeau, Vice President, Online
Susan Cardoza, National Sales Director, Integrated Solutions
Scott Buckler, Director of Integrated Solutions
Stephanie Gutierrez, Online Acct. Manager, Integrated Solutions
Michael Hiatt, Director of Integrated Solutions
James Kalbach, Director of Integrated Solutions
Debbie Lovell, Online Account Manager, Integrated Solutions
Kate Zinn, Director of Integrated Solutions
Denise Lendry, Sales Coordinator
Lisa Thompson, Sales Coordinator
Internet: knormandeau, scardoza, sbuckler, sgutierrez, mhiatt, jkelbach, dlovell, kzinn, dlandry, lthompson@nww.com
(508) 460-3333/FAX: (508) 861-0467

MARKETPLACE/EMERGING MARKETS
Donna Pomponi, Director of Emerging Markets
Enku Gubaie, Manager of Marketplace/Emerging Markets
Caitlin Horgan, Manager of Marketplace/Emerging Markets
Jennifer Moberg, Manager of Marketplace/Emerging Markets
Chris Gibney, Sales Operations Coordinator
Internet: dpomponi, egubaie, chorgen, jmoberg, cgibney@nww.com
(508) 460-3333/FAX: (508) 460-1192

CTIA
continued from page 1

security," says Ellen Daley, principal analyst at Forrester Research. "Do I allow devices that somebody just buys to connect to my network? Are they compliant from an operating system and application perspective? Do I scan and quarantine them if they don't comply?"

Another consideration is whether the devices enable seamless roaming between the company and carrier network, or between different carrier networks. Many large corporations are deploying IEEE 802.11 Wi-Fi wireless LANs internally, while the wireless WAN is migrating from 2G and 2.5G standards to 3G technologies.

Ensuring a consistent user experience and level of service is a challenge.

"An often overlooked point is that enterprises are still in a three-, four- or five-carrier environment," says Michael Voellinger, vice president of wireless services for Telwares, a telecom consultancy. "You need to look at where the market and technology is going, and who you are working with. You need a consistent platform and experience."

Dual-mode Wi-Fi/cellular mobile devices exist, but they are costly and have a shorter battery life because they support two radio antennas — one for Wi-Fi and the other for the particular cellular technology employed by the carrier. And if that cellular technology is 2G or 2.5G, the handset could become obsolete if users want to take full advantage of the 3G capabilities coming from their carrier.

Obsolescence is par for the course for Nova-Sol, a government contractor in Hawaii with a mobile workforce.

"The life span of a cell phone is a year anyway," says Jim Miller, director of technical resources. "But we don't have to throw 80 away and buy 80 new ones, because not everyone needs the latest and greatest."

But Wi-Fi-to-cellular handoff might introduce transmission delays, which would disrupt a service such as mobile VoIP, considered one of the upcoming killer applications for untethered corporations.

Intel is grappling with these issues. The company is embarking on a mobile VoIP project for a 5,000-worker campus that encompasses Wi-Fi within the company and Wi-Fi/3G/WiMAX in the wide area. "Open questions" regarding mobile VoIP include QoS, roaming and security, says Joaquin Sufuentes, director of e-Business and IT in the wireless networking group at Intel.

"How do you secure something that crosses networks?" he asks.

Complicating matters is that Wi-Fi security standards are still in flux. Wi-Fi Protected Access, which uses Temporal Key Integration Protocol encryption, is evolving into 802.11i, which uses Advanced Encryption Standard. And on the horizon is 802.11r, which is intended to enable fast, secure handoff between Wi-Fi access points to overcome the delay and QoS degradation inherent in authentication.

Intel also is investigating user/device-to-access point coverage characteristics and requirements for mobile VoIP, an issue that hits home with other mobile users.

Airing concerns

Mobile issues facing corporations include:

- Multi-radio handsets consume battery life, which increases cost.
- Handsets have to be managed as any other asset.
- Establishing and enforcing policies on business and personal use.
- Ensuring secure, service-guaranteed mobility between Wi-Fi and cellular networks.
- Securing the mobile network without degrading QoS.
- Coverage, especially for mobile VoIP.

RKA Petroleum Companies in Romulus, Mich., uses BlackBerry e-mail devices and GPS on a Nextel service to communicate with its fleet of truck drivers.

The system is fine for wireless e-mail but slow for opening server or database files, says Jason Hittleman, vice president of IS at RKA. The company is evaluating higher-speed — 11M and 54M bit/sec — Wi-Fi service but hasn't deployed it because of coverage gaps, he says.

"When you look out there, there are still a lot of dead spots, still a lot of open space," Hittleman says. Lack of ubiquitous coverage also tables any plans the company might have for mobile VoIP. ■

Wireless
Subscribe to our free newsletter.
DocFinder: 5434 www.nwfusion.com

Kazeon's storage appliance handles unstructured data

■ BY DENI CONNOR

Kazeon Systems says it is set to introduce a storage appliance that not only analyzes the unstructured data on file servers but also decides where to store that data, and determines who can retrieve it and when, based on rules that IT creates.

The company, founded in 2003 by Sudhakar Muddu and three other storage veterans from Broadcom, AT&T and Sprint, joins a slew of others mining data for its content, and making decisions on how and where it will be stored. Muddu was the founder of Sanera, which he sold to McData in 2003 for $102 million.

Identifying, managing and auditing the unstructured data on a network for compliance and security purposes is a large and growing market. Unstructured content — files, e-mails, non-transactional data and medical images — accounts for 80% of the data on a network, Enterprise Strategy Group says.

"Companies have begun to recognize the risk that is created by unmanaged information in the enterprise, be that compliance issues or litigation exposure or even just making bad decisions," says Troy Toman, vice president of marketing at Kazeon.

Companies such as StoredIQ (formerly Deepfile), Arkivio, Abrevity and Scentric, which is still in stealth mode, make appliance-based software that classify data and storage resources into logical groups based on administrator-defined criteria for efficient data retention. Often, these appliances will sit in or next to the data path between file servers on a network and devices such as EMC's Centera or Network Appliance's NearStore R200 systems, which store unstructured data.

"The way to think of [Kazeon's appliance] is as an intelligent information platform that sits in front of an archiving solution like EMC's Centera," says Brad O'Neill, senior analyst for Taneja Group. "The policies the IT manager creates could control encrypting that data, moving it to an archival device or restricting access to it."

Kazeon's Linux-based appliance discovers and analyzes Microsoft's Common Internet File System and the Unix/Linux Network File System data. It is similar to StoredIQ 3.0, which is designed to discover and manage data for compliance with the Health Insurance Portability and Accountability Act. Taking a different approach is Arkivio's Auto-Stor, which isn't content-aware. Auto-Stor is more of a data management application that cracks open and analyzes files so they can be managed more easily.

Kazeon's yet-to-be named appliance is in beta and is expected to ship by midyear. The company is funded for $17 million by Redpoint Ventures, Clearstone Venture Partners and Goldman Sachs. ■

Data overload

A slew of companies are popping up to address the management of unstructured data.

Company/product	Function	Benefits
Abrevity Network File Management	Data management	Lets IT scan files on a network to improve storage utilization.
Arkivio Auto-Stor	Data management	Lets IT migrate and access data for compliance or archival purposes.
Kazeon Systems, as yet unnamed	Content-aware data management	Lets IT determine how information is stored and retrieved and who can access it.
Scentric, as yet unnamed	Data management	Lets IT migrate and access data for compliance or archival purposes.
StoredIQ 3.0	Content-aware data management specifically for HIPAA	Lets IT determine how HIPAA information is stored and retrieved and who can access it.

■ **Network World**, 118 Turnpike Road, Southborough, MA 01772-9108, (508) 460-3333.

Periodicals postage paid at Southborough, Mass., and additional mailing offices. Posted under Canadian International Publication agreement #40063800. Network World (ISSN 0887-7661) is published weekly, except for a single combined issue for the last week in December and the first week in January by Network World, Inc., 118 Turnpike Road, Southborough, MA 01772-9108.

Network World is distributed free of charge in the U.S. to qualified management or professionals.

To apply for a free subscription, go to www.subscribenw.com or write Network World at the address below. No subscriptions accepted without complete identification of subscriber's name, job function, company or organization. Based on the information supplied, the publisher reserves the right to reject non-qualified requests. Subscriptions: 1-508-490-6444.

Nonqualified subscribers: $5.00 a copy; U.S. - $129 a year; Canada - $160.50 (including 7% GST, GST#126659952); Central & South America - $150 a year (surface mail); Europe - $205 a year (surface mail), all other countries - $300 a year (airmail service). Four weeks notice is required for change of address. Allow six weeks for new subscription service to begin. Please include mailing label from front cover of the publication.

Network World can be purchased on 35mm microfilm through University Microfilm Int., Periodical Entry Dept., 300 Zebb Road, Ann Arbor, Mich. 48106.

PHOTOCOPYRIGHTS: Permission to photocopy for internal or personal use or the internal or personal use of specific clients is granted by Network World, Inc. for libraries and other users registered with the Copyright Clearance Center (CCC), provided that the base fee of $3.00 per copy of the article, plus 50 cents per page is paid to Copyright Clearance Center, 27 Congress Street, Salem, Mass. 01970.

POSTMASTER: Send Change of Address to **Network World**, P.O. Box 3090, Northbrook, IL 60065. Canadian Postmaster: Please return undeliverable copy to PO Box 1632, Windsor, Ontario N9A7C9.

BPA INTERNATIONAL BPA TAG

Copyright 2004 by Network World, Inc. All rights reserved. Reproduction of material appearing in Network World is forbidden without written permission.

Reprints (minimum 500 copies) and permission to reprint may be purchased from Reprint Management Services at (717) 399-1900 x124 or rtry@rmsreprints.com.

USPS735-730

Nortel

continued from page 1

encompasses the BayStack switch line. The Ethernet Routing Switch 8600 Version 4.0 will be based on the Passport chassis with a new management module that can boost total switch capacity to 720G bit/sec, up from 520G bit/sec on the Passport 3.X versions.

New service blades for the 4.0 switch will include a three-port 10G Ethernet module; an upgrade from the single-port 10G blade was available with the 3.X series Passports. Also on tap is a 30-port Gigabit Ethernet module with interchangeable fiber/copper small form factor pluggable ports. A copper-based, 48-port 10/100/1000M bit/sec blade also is scheduled to be released. All these products are set to be launched next month. Pricing has not been set.

The switch gear was three years in the making, Nortel says, as the company revamped the architecture for its line cards and switch fabric modules, changing the way these components handle packet forwarding and processing.

"We really built this switch to run multimedia applications," says Atul Bhatnagar, Nortel vice president and general manager of Ethernet Switching Business. On the service modules, he says, re-programmable network processors now are used instead of ASICs for Layer 2-4 switching and traffic handling. Whereas ASIC logic is burned into hardware, the network processor approach lets the switch be tweaked for speeding up applications such as voice and video, or for adding security features. For example, network processors could be changed to optimize how specific protocols perform in hardware, such as Session Initiation Protocol. Also, as new viruses and worms evolve, the latest rules to prevent this code from running through a LAN could be added to the switch gear, Bhatnagar adds.

The switch technology also will include Ethernet Routing Switch 4.0 operating system software, and an upgraded 720G bit/sec switch fabric — the 8692 switch fabric module, released last year. An upgraded power supply also is needed for the switch to reach its new bandwidth capacity. Dual 8692s can be deployed in a Ethernet Routing Switch 8600 to scale to 1.44T bit/sec.

Two 8600 chassis can be linked with Nortel's Split Multi-Link Trunking technology, so core switches share traffic streams from a LAN aggregation layer. This creates a multi-terabit core and provides sub-second failover, Nortel says.

"Nortel provided the best overall value, in terms of meeting our functionality requirements, as well as cost," says Ed Shikata, San Jose's deputy city manager.

The re-bidding process was restarted last fall after an audit of the Cisco network bid found that city IT staff had worked closely with Cisco for technology selection, which is against city regulations. Cisco engineers and account managers worked with the city's IT staff to design network requirements that would let only Cisco-based LAN, VoIP and security gear be used, the report said.

With the Nortel-based contract, the vendor is challenged with a short turnaround; it must have the network up and running by June 9, when the new city hall is due to open. If the deadline is not met, Nortel will owe the city $20,000 per day. A $1.6 million chunk of the deal will go toward one year of managed services from Nortel.

The deal includes Nortel backbone, aggregation and wiring closet switches in the LAN. Nortel Alteon firewall and Contivity VPN/router equipment will be deployed to connect the city hall network to external WAN links, remote-access users and the Internet. The VoIP gear includes redundant Nortel Communication Server 1000 IP PBXs, running IP phones and soft-phone applications. A Nortel Multimedia Communication Server 5100 will be deployed, letting users access unified messaging, voice and video-conferencing applications and presence management software.

The Nortel switches going into the new San Jose City Hall would be a welcome addition at another government agency.

"We could use that kind of bandwidth," says Sheng Guo, CTO for the New York State Unified Court System, which runs more than 80 older-generation Passport 8600 switches in 60 courthouses. Guo says the court system is rolling out a live recording system for its network of more than 100 IP video cameras. "Bringing these cameras online is going to take a large chunk of my bandwidth," he says. Each camera streams 4M bit/sec of video — times 100 cameras, so this would eat up half the 1G bit/sec links that connect the court's facilities over dark fiber.

"Ten Gigabit would be an obvious remedy for that," he says.

Nortel was on the forefront of pre-standards 10G Ethernet, introducing single- and dual-port 10G blades for the Passport 8600 in 2002. But these products ran on older architecture, which allowed only up to 8G bit/sec of throughput per port. Since 2003, Nortel's high-performance switch rivals all have released products with higher capacity and 10G blades in the four- to six-port range, with support for full 10G bit/sec on ports.

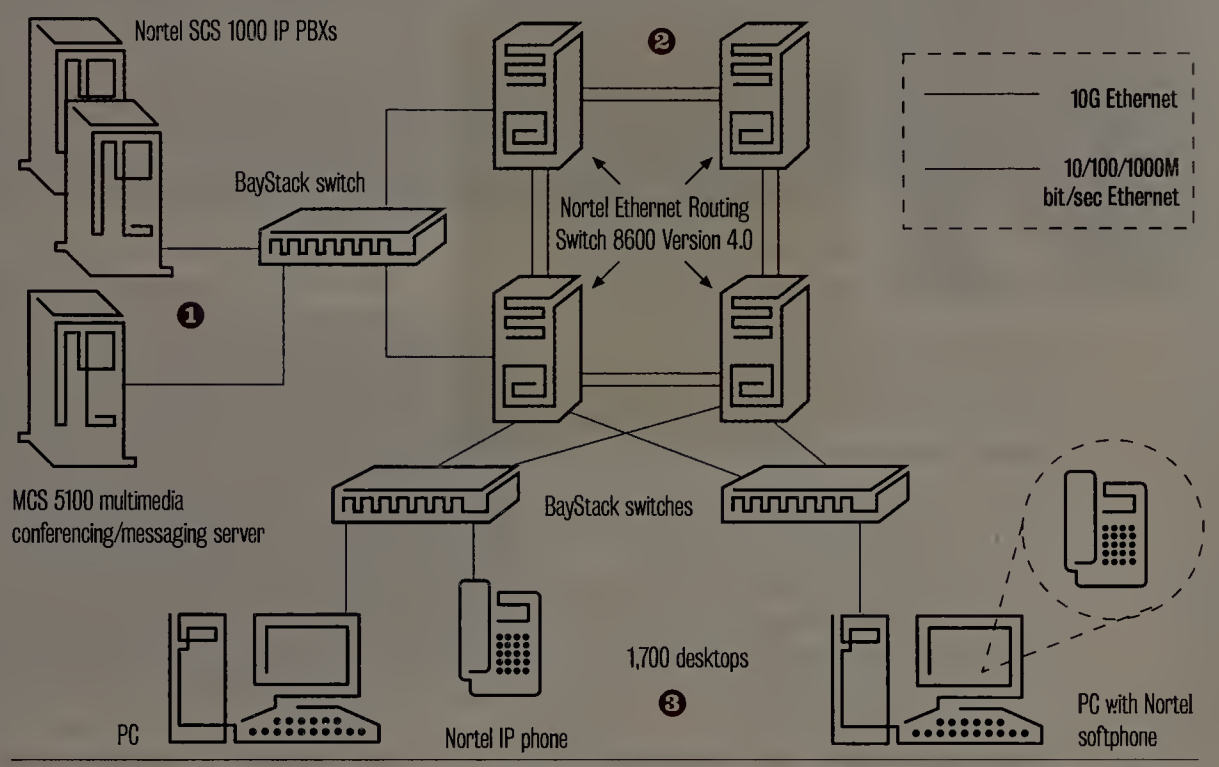
"Nortel often comes on in waves," says Steven Schuchart, an analyst at Current Analysis. "They had some of first the 10G switching technology, but follow-up has been a problem for them."

In terms of pure bandwidth and scale, Nortel's new gear is not as high-powered as that of Cisco, Enterasys Networks, Extreme, Force10 or Foundry. But the San Jose deal gives Nortel one of the most high-profile enterprise customer deployment efforts with 10G, as many rival customer announcements have focused on research institutions with high-performance computing and clustering deployments.

"Nortel is still the only other Tier 1 player in the enterprise market," besides Cisco, Schuchart says. "If a large company has a problem with Cisco ... Nortel is who they turn to because of its size and age and stability." ■

Downtown upgrade

The new San Jose City Hall is getting a converged network based on Nortel IP PBXs and the vendor's latest 10G backbone switch.



1. Nortel Succession Communication Server 1000s — IP PBXs — will operate the voice network, and interoperate with multimedia conferencing and presence applications on an MCS 5100 messaging server.
2. The network will be built on Nortel's forthcoming Ethernet Routing Switch 8600 Version 4.0, with 10G Ethernet trunks and Split MLT technology, letting the core act as a single virtual switch.
3. More than 1,700 users with converged desktop applications will connect to the LAN via 10/100/1000M switched Ethernet.

Zultys launches new IP phones

■ BY PHIL HOCHMUTH

Zultys Technologies this week will launch five Session Initiation Protocol-based IP phones with an array of feature combinations for various deployments.

The phones, all under Zultys' ZIP 2 brand, include two devices aimed at desktops, with graphical LCD screens, data encryption and speakerphones. The other three are basic-feature IP phones.

The phones operate with Zultys' MX250 or MX1200 line of SIP-based IP PBXs. The phones also can work with other IP telephony gear that supports SIP.

The ZIP 2x1 and ZIP 2x2 are targeted at business desktops and are capable of displaying GUI-based interfaces. The phones also include screen menus and encryption of voice and SIP signaling traffic. The 2x2 model can be powered via 802.3af Power over Ethernet (PoE) and includes a two-port Ethernet switch for connecting a PC and phone to the LAN via a Category 5, 5e or 6 network drop.

The ZIP 2+, 2P and 2x2L phones have text-only LCD displays and do not support encryption. Users looking for a basic-feature phone with PoE support can choose the ZIP 2P. Like the ZIP 2x2, the 2x2L includes a dual-port switch for linking a PC and phone but does not include PoE support.

The ZIP 2 phones join Zultys' 4x4 line of IP phones, which include four-port Ethernet switches and support up to four lines for conference calling.

The new ZIP 2 phones probably will be the IP endpoint of choice going forward at one Zultys site — Canby Builder Supply in Portland, Ore.

The 80-employee building supply company uses the Zultys MX250 IP PBX and ZIP 4x4 phones.

"The 4x4 phones are nice, but they're kind of overkill for what we need," says Alan Churchill, director of MIS for Canby. He says the pricing of the ZIP 2 series — $150 to $230, depending on the model — is also attractive. (The average price for an IP phone in 2004 was about $320, according to IDC.)

Zultys competes with small-office IP PBX vendors such as 3Com, Altigen, EADS Telecom and Sphere, and larger vendors with small-office VoIP wares, including Avaya, Cisco, Nortel and Siemens. ■

BackSpin Mark Gibbs

SBC makes DSL, er, exciting

As some of you might remember from previous columns, I have been involved in getting my son's school online and computerized. A few weeks ago the school called me because their e-mail services had suddenly stopped working: Although they could receive e-mail, no one could send anything.

We'd had some previous problems with the server but a simple restart fixed them. No luck this time around. I tried sending and receiving e-mail from the server and it appeared that the POP3 service was running, but the SMTP service wouldn't respond. To this day, I do not know why it failed.

If it hadn't, this story would be a lot shorter.

So I e-mailed the server's owner and he restarted it, and e-mail then appeared to work. I told the school the next day and they called me back minutes later to say that nope, still didn't work for them.

Now at this point I was pushed for time so I e-mailed the server's owner again and got him to refer the problem to his support people. Two days later (which was just over a week into the school not having e-mail) I chased it down and found out that he'd never heard back from support.

Because of this and a couple of other problems we'd had with the server, all of which seemed to be caused by the server being somewhat antique (a Cobalt RAQ), I decided to move the school's Web site and e-mail to another server.

The school's principal told me that another parent had offered his server so I worked with him and a few days later the new accounts were set up. But as far as the school was concerned the e-mail system was still dead in the water.

My story solved

Well, to make a long IT story (is there any other kind?) short, I went back to the school and started trying to figure out what was going on. A bit of poking around revealed that no servers on the Internet could be contacted on Port 25, the port used for SMTP. Obviously, Port 25 was being blocked ... but why?

No, surely not ... but there it was: A Google search revealed that SBC, the school's DSL provider, had decided, in its wisdom, to stem the flow of spam by blocking SMTP! Turns out that SBC rolled out this ridiculous and ineffective program sometime late last year but only for accounts using dynamic IP addresses. As I have a static address Port 25 blocking hadn't affected me. To find out about the blocking you had to be psychic or read the notice sent to the SBC e-mail account the company provides when you install your DSL line.

But if you use some other e-mail service all you'll find in the SBC account are SBC marketing messages, so I suspect most people ignore it. Even better, it turns out that the school's account isn't accessible any longer for reasons that I have yet to determine.

To unblock Port 25 you have to go to SBC's "Abuse of Service" Web page and request to be unblocked using a poorly designed form. A couple of hours later, and after roughly three weeks of being disconnected, the school was sending and receiving e-mail.

This has to be one of the most ill-conceived anti-spam tactics I've come across. SBC seems to have hardly thought through the issues. Did it send out a notice with its service invoice? Not that I saw. Did it check whether DSL customers actually use their accounts or that the accounts even work? Apparently not.

But worst of all, not only was the blocking plan badly executed, it also would hardly be a deterrent for serious spammers — they would just use a different port to transfer mail to a remote mail server.

Thanks SBC for making everyone's life just a little more exciting.

Excited? Tell backspin@gibbs.com and let's talk it over on Gearblog (www.nwfusion.com, DocFinder: 6344).

'NetBuzz News, insights, opinions and oddities

By Paul McNamara

Metcalfe's Law . . . ain't?

Math has never been my strong suit, so far be it from me to get between industry legend Bob Metcalfe and a pair of university researchers as they butt heads over the validity of "Metcalfe's Law."

Actually, it's the academics doing most of the head knocking; Metcalfe is more or less bemused by the attention.

Andrew Odlyzko and Benjamin Tilly of the Digital Technology Center at the University of Minnesota earlier this month dissed Metcalfe's theory but good in a paper titled "A refutation of Metcalfe's Law and a better estimate for the value of networks and network interconnections." You can access the paper and read the blow-by-blow at www.nwfusion.com, DocFinder: 6342.

Metcalfe's Law posits that the value of a network grows proportionally with the square of its number of users. Meant to be more descriptive than taken literally, it first surfaced in a slide presentation Metcalfe gave in the early 1980s when he was running 3Com and gained acclaim in the late 1990s as justification for "hockey stick" growth projections that propped up many a revenue-barren dot-com.

"The fundamental fallacy underlying [Metcalfe's Law] is in the assumption that all connections or all [enabled] groups are equally valuable," Odlyzko and Tilly argue in their paper.

Even a guy living in a shack out in the woods — without a phone, never mind broadband — ought to appreciate this point, they say.

"The defect in this assumption was pointed out a century and a half ago by Henry David Thoreau. In *Walden,* he wrote: 'We are in great haste to construct a magnetic telegraph from Maine to Texas; but Maine and Texas, it may be, have nothing important to communicate."

Odlyzko and Tilly do offer an alternative to Metcalfe's Law, suggesting that "the value of a general communication network of size n grows like $n \log(n)$."

In terms even a journalism major can understand, they're saying the value of combined networks do exceed the mere sum of their parts, but by a dramatically more modest amount than Metcalfe's Law has led adherents to believe.

"The problem is that Metcalfe's Law provides irresistible incentives for all networks relying on the same technology to merge or at least interconnect. . . . Yet historically there have been many cases of networks that resisted interconnection for a long time," the Minnesota researchers say. They cite a number of examples, with the most recent being stubbornly proprietary instant-messaging networks that have only recently shown any meaningful willingness to play well with others.

As for Metcalfe, he appears none too concerned by the academics' assault on his famous theory.

"I am delighted that Metcalfe's Law keeps getting all this attention," says Metcalfe, a general partner at Polaris Venture Partners who earlier this month received the National Medal of Technology from President Bush.

"Unlike Moore's Law, which has been numerically true since 1965, Metcalfe's Law has never been numerically true, unless you allow me to adjust the constant of proportionality to fit each case," he says.

"One trouble is that the 'value' of networking is very hard to measure," adds Metcalfe, whose twinkle in discussing the matter is evident even via e-mail. "So now that Metcalfe's Law is debunked, what is the exact formula for the value of a network?"

My best guess would have something to do with angels dancing on the head of a pin, but no one's asking me.

"I still think it is a terribly good idea to connect things," Metcalfe continues. "And merging disconnected networks is a great idea.

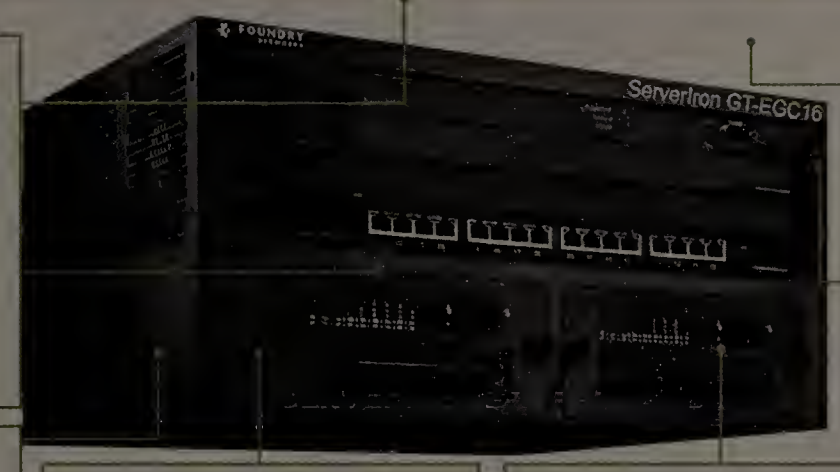
"Huge monopolies, on the other hand, are a bad idea," he adds.

And it's also another idea that appears to be out of favor these days.

Want to lay down a law of your own? The address is buzz@nww.com.

ServerIronGT E-Series Takes Application Switching to New Heights

Doing Things That PC Appliances Cannot



High Availability & Reliability

- Resilient switching and routing foundation
- Global load balancing for multi-site scalability and survivability
- Link aggregation
- Rapid and stateful session failover
- RSTP, VRRP for switch and router redundancy
- Redundant power supplies

Security

- DoS protection up to 4 million SYN/sec
- Wire-speed ACLs
- Application rate limiting
- Secure device management
- sFlow traffic monitoring

Rich Features

- Intelligent content switching using URL, HTTP, XML, cookies, SSL ID and others
- IP NAT
- RIPv2, OSPF routing

Flexibility & Manageability

- In-line, one-ARM and Direct Server Return modes
- Web, SNMP, INM and Cisco-like CLI

Superior Performance

- Up to 140,000 L4 connections/sec
- Application throughput from 2 to 12 Gbps
- Wire-speed Layer 2/3 forwarding
- Scalable processor performance

Scalability & Expandability

- Port expansion to:
  - 48 Gigabit Ethernet
  - 48 10/100 Mbps Ethernet
  - 4 10-Gigabit Ethernet

Uptime, scalability, performance and security are the watchwords for your network. The ServerIron® application switch is designed for this environment. Its advanced switch-based architecture features a scalable content switching engine with hardware-based DoS protection delivering the industry's most powerful and secure application switching solution.

PC Appliances Cannot Match the Power and Flexibility of the ServerIron

	ServerIron	PC Appliances
Performance upgradeability	✓	X
In-service port expandability	✓	X
10-GE support, >10 Gpbs throughput	✓	X
High-density direct server fan-out	✓	X
Hardware-based connection management and DoS protection	✓	X
Wire-speed L2/L3 forwarding and ACLs	✓	X

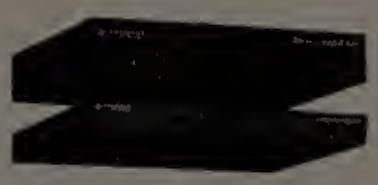
FOUNDRY® NETWORKS

The Power of Performance™

The ServerIron Family of Products Also Includes:

ServerIron 450 and 850

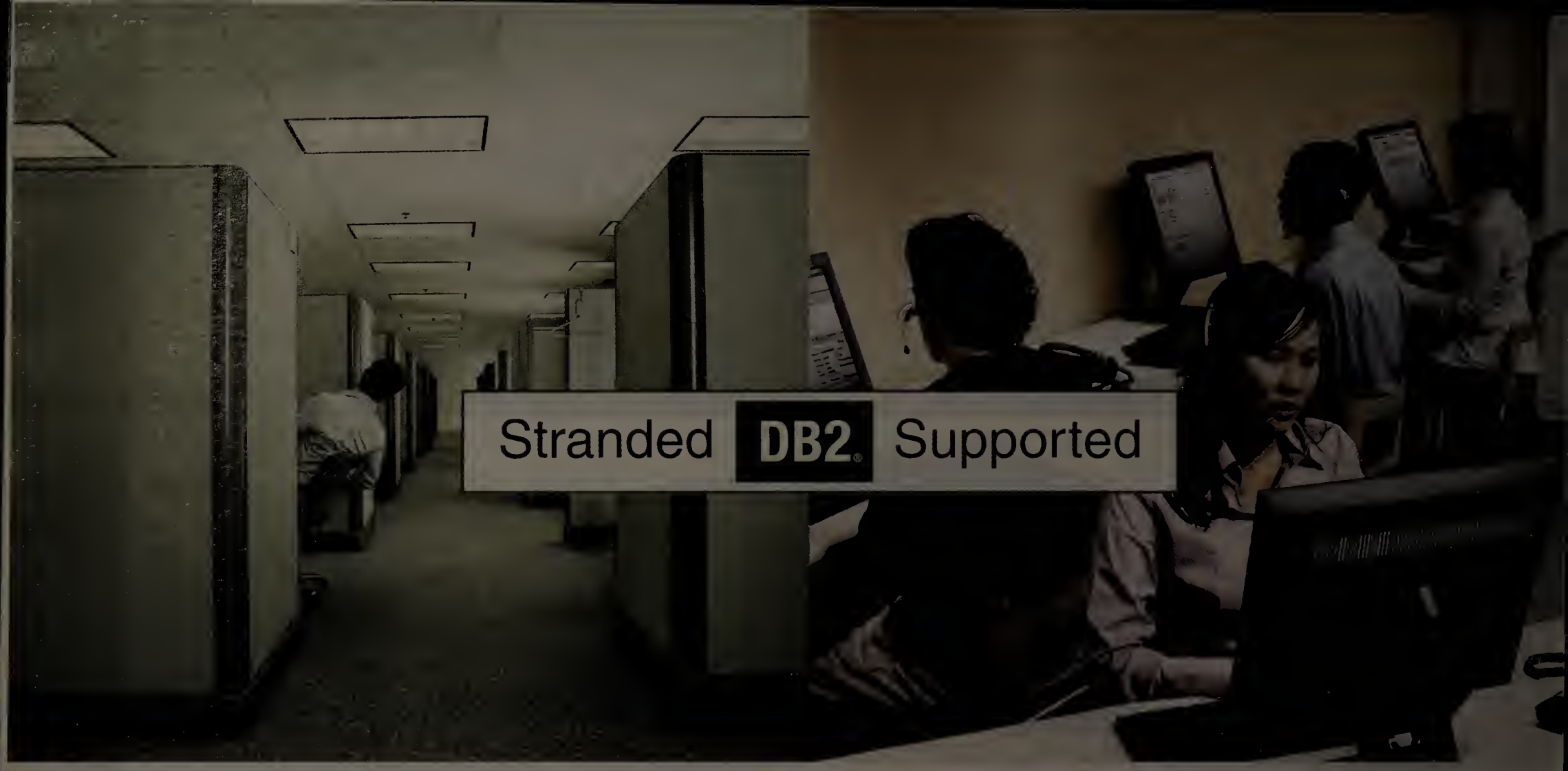
ServerIronXL



ServerIronSA Accelerators

Foundry Networks, Inc. is a leading provider of high-performance Enterprise and Service Provider switching, routing and Web traffic management solutions including Layer 2/3 LAN switches, Layer 3 Backbone switches, Layer 4–7 Web switches, wireless LAN and access points, access routers and Metro routers.

For more information please call: US/Canada 1 888 TURBOLAN, International +1 408.586.1700 or visit our website at www.foundrynet.com/sie



DB2 WON'T ABANDON YOU.

Perhaps you've heard: Oracle desupported Oracle Database 8i last year. Meaning potential headaches, higher cost or a complete migration to current versions of Oracle. Fortunately, IBM offers ongoing, around-the-clock service and support for DB2.

But that's not all. A Solitaire study has found that, on average, Oracle Database requires 25% more time to manage than DB2.[1] That's big.

And an ITG study showed overall costs for Oracle Database up to four times higher than DB2.[2] The Transaction Processing Performance Council results show that DB2 and eServer™ p5-595 are more than twice as scalable as Oracle Real Application Clusters, making them the overwhelming performance and scalability leader for TPC-C.[3] That's big, too.

No wonder DB2 is regarded as the leading database built on and optimized for Linux,® UNIX® and Windows.® Like other IBM database engine products such as Informix® and Cloudscape,™ DB2 is part of an innovative family of information management middleware that integrates, and can actually add insight to your data.

It's also built to take full advantage of your existing heterogeneous and open environments, and is built to enable true grid computing.

Why not move up to middleware that makes sense? Now you can get IBM DB2 Universal Database or Informix by taking advantage of our extremely compelling trade-up program. Visit **ibm.com**/db2/swap today to find out if you qualify.

IBM

ON DEMAND BUSINESS™

IBM, the IBM logo, DB2, eServer, Informix, Cloudscape and the On Demand logo are trademarks or registered trademarks of International Business Machines Corporation in the United States and other countries. Linux is a registered trademark of Linus Torvalds. Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and/or other countries. UNIX is a registered trademark of The Open Group in the United States and/or other countries. Other company, product and service names may be trademarks or service marks of others. © 2005 IBM Corporation. All rights reserved. [1]"DB2 Performance on IBM Server® pSeries and xSeries," Solitaire Interglobal Ltd., 2003: based on Oracle Database 9i. [2]"IBM Solutions for PeopleSoft Deployment in Mid-sized Businesses Quantifying the New Cost/Benefit Equation," July 2003, International Technology Group, Los Altos, California. [3]All referenced results are current as of 12/14/04. DB2 UDB v8.2 on IBM eServer p5 595 (64-way POWER5 1.9 GHz) and AIX 5.3L: 3,210,540 tpmC @ $5.19/tpmC available: May 15, 2005, vs. Oracle RAC 10g on HP Integrity rx5670 Cluster 64P (16 x 4-way Intel Itanium2 6M 1.5GHz): 1,184,893 tpmC @ $5.52/tpmC available: April 30, 2004; TPC Benchmark, TPC-C, tpmC are trademarks of the Transaction Processing Performance Council. For further TPC-related information, please see http://www.tpc.org/